Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Bijlagen bij de Vraagspecificatie

(Prestatiecontract)

Het meerjarig in stand houden van, monitoren van en informeren over de toestand van het Areaal, met upgradewerkzaamheden, in het beheergebied van Rijkswaterstaat Zee & Delta, district Noord.

Datum: 10 oktober 2019

Zaaknummer: 31137096

Colofon

Uitgegeven door	Ministerie van Infrastructuur en Waterstaat, Rijkswaterstaat Programma's, Projecten en Onderhoud
Datum	10 oktober 2019
Status	Concept
Versienummer	V0.3

Vertrouwelijkheid: RWS INFORMATIE

Inhoud

	Inleiding	**5**
Bijlage A	**Informatie Areaal**	**9**
Bijlage B	**Levering areaalgegevens**	**14**
Bijlage C	**Calamiteiten, incidenten en schadeherstel**	**22**
Bijlage D	**Werkbare Uren (WBU)**	**31**
Bijlage E	**Slot's**	**32**
Bijlage F	**Aanvragen verkeersmaatregelen**	**33**
Bijlage G	**Overzicht ten behoeve van Activiteiten**	**34**
Bijlage H	**Projectrisicolijst**	**37**
Bijlage I	**Reinigen van zeer open asfaltbeton**	**38**
Bijlage J	**Beoordelingsmethodiek schade bovenbouw en onderbouw**	**39**
Bijlage K	**Integraal Veiligheidsplan**	**44**
Bijlage L	**Definities integrale veiligheid**	**45**
Bijlage M	**Regelingenschema Kabels en Leidingen Derden**	**46**
Bijlage N	**Richtlijn Samenwerking Rijkswaterstaat - Markt op Integrale Projecten**	**49**
Bijlage O	**Rijkswaterstaat Brede Afspraak Archeologie**	**50**
Bijlage P	**Programma van Eisen voor uitvoerend archeologisch onderzoek**	**51**
Bijlage Q	**Rijkswaterstaat Brede Afspraak Duurzaam Inkopen**	**52**
Bijlage R	**Staat van prijzen per eenheid calamiteiten en incidenten**	**53**
Bijlage S	**Melding inzet zelfstandige hulppersoon**	**59**
Bijlage T	**Coördinatie van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen**	**60**
Bijlage U	**Informatievoorziening ter plaatse bij verkeersmaatregelen ten behoeve van wegwerkzaamheden**	**67**
Bijlage V	**Richtlijnen Cybersecurity**	**68**
Bijlage W	**Invulinstructie format LV BRO**	**125**
Bijlage X	**Richtlijnen voor inspectie en onderhoud van faunavoorzieningen bij wegen 2008.**	**127**

Bijlage Y Quick Reference Card Wekelijkse Rapportage 128

Bijlage Z Inspectie waterkeringen in het kader van de Zorgplicht Waterveiligheid129

Bijlage AA Verkeersmanagement voor werk in uitvoering op Rijkswegen 130

Bijlage AB Specificatie Functionele Inspecties en Testen 131

Bijlage AC FIT_Typical (Generieke FIT-lijst) 132

Bijlage AD Specificatie NEN3140 en NEN3840 inspecties 133

Bijlage AE Faaldefinitiecategorieën 134

Bijlage AF Industriële automatisering 135

Vertrouwelijkheid: RWS INFORMATIE

Inleiding

Deze bijlagen maken onderdeel uit van de Vraagspecificatie behorende bij de Overeenkomst.

1. Leeswijzer

De bijlagen zijn een aanvulling op de eisen en bepalingen in de Vraagspecificatie, waarbij de bijlagen in een aantal groepen kunnen worden ingedeeld:

- gegevens betreffende het Areaal, die relevant zijn voor het Meerjarig Onderhoud, het Werk en/of de Werkzaamheden;
- risico's betreffende het project;
- nadere en aanvullende eisen en bepalingen met betrekking tot het Meerjarig Onderhoud, het Werk en/of de Werkzaamheden;
- kaders en richtlijnen, die door Rijkswaterstaat worden gehanteerd en van toepassing zijn op de Overeenkomst;
- regionale bijlagen.

De regionale bijlagen bevatten eisen en bepalingen die specifiek voor de regio of een deel daarvan gelden, waar de Overeenkomst betrekking op heeft. Deze kunnen per contract verschillen maar zijn altijd aanvullend op de algemene eisen, bepalingen en bijlagen.
In de Vraagspecificatie Eisen staat de relatie en hiërarchie van de diverse eisen, bepalingen en documenten beschreven.

De bijlagen hebben allemaal een bijlageletter en -titel, waarnaar vanuit de diverse delen van de Vraagspecificatie en de Basisovereenkomst wordt verwezen. In de volgende paragraaf is een referentielijst opgenomen, waarin deze relaties zijn aangegeven, zodat vanuit de bijlagen ook de bijbehorende eisen zijn te vinden.
De bijlagen A tot en met AE zijn standaard voor wat betreft de structuur, indeling en tekst, waarbij een aantal gegevens wel regiospecifiek is ingevuld. De overige bijlagen zijn regio- of projectspecifieke bijlagen.

2. Referentielijst

Onderstaande referentielijst geeft een overzicht van de documenten waarnaar vanuit eisen wordt verwezen en die als bijlage bij de Vraagspecificatie zijn opgenomen , op internet beschikbaar zijn, bij CROW aangeschaft kunnen worden en anders apart zijn verstrekt.

Omschrijving referentie	**Vraagspecificatie deel**	**Eis / bepaling**	**Bijlage bij de Vraagspecificatie**
Levering areaalgegevens (inclusief alle documenten die genoemd zijn in bijlage B "Levering areaalgegevens" van de Vraagspecificatie, ook indien elders in Vraagspecificatie genoemd)	Proces	US220 OP120 OP220	B
NEN-EN-ISO 9001; vigerende versie, beschikbaar op internet	Proces	KM020	-
Projectrisicolijst	Proces	RM110	H
Integraal Veiligheidsplan	Proces	RM110	K
Definitie Integrale Veiligheid	Proces	B-VH020	L

Omschrijving referentie	Vraagspe-cificatie deel	Eis / be-paling	Bijlage bij de Vraag-specificatie
Regelingenschema Kabels en Leidingen Derden	Proces	B-KL100	M
CROW-publicatie 500 "Schade voorko-men aan kabels en leidingen, Richtlijn zorgvuldig grondroeren van initiatief- tot gebruiksfase" d.d. 2 november 2016 ISBN 978 90 6628 658 verkrijgbaar via CROW, zie www.crow.nl	Proces	KL210	-
Werkbare Uren (WBU), Venstertijden Afsluitingen (VTA) en werkvensters	Proces	B-VM710 B-VN420 UA350	D
Slot's	Proces	B-VM320 B-VN450	E
Aanvragen verkeersmaatregelen	Proces	VN600 VN630 VN800	F
Richtlijnen Vaarwegen - RVW 2017 (§8.4 Beperken hinder) d.d. december 2017 , zie http://www.rws.nl/zakelijk/werken-aan-infrastructuur/bouwrichtlijnen-infrastructuur/vaarwegen.aspx	Proces	VN300	-
Richtlijnen Scheepvaarttekens (RST 2008) RWS Dienst Verkeer en Scheepvaart, d.d. december 2008 ISBN 978-90-369-3638-5 zoals gepubliceerd op https://staticresources.rijkswaterstaat.nl/binaries/Richtlijnen%20Scheepvaarttekens%20-%20RST%202008_tcm174-272349_tcm21-20430.pdf	Proces	VN300	-
Archeologische MonumentenKaart (AMK) van de Rijksdienst voor het Cultureel Erfgoed (RCE), zie https://geoservices.rijkswaterstaat.nl/ext/geoweb51/index.html?viewer=ArcheologischeTerreinenInfra.Webviewer	Proces	AW020	-
Rijkswaterstaatskaart AMK-terreinen met een hoge archeologische waarde, zie https://geoservices.rijkswaterstaat.nl/ext/geoweb51/index.html?viewer=ArcheologischeTerreinenInfra.Webviewer	Proces	B-AW040	-
Herkennen van archeologische vondsten uit waterbodems en hoe daar mee om te gaan, zie https://www.cultureelerfgoed.nl/publicaties/publicaties/2013/01/01/herkennen-	Proces	AW070	-

Vertrouwelijkheid: RWS INFORMATIE

Omschrijving referentie	Vraagspecificatie deel	Eis / bepaling	Bijlage bij de Vraagspecificatie
van-archeologische-vondsten-uit-waterbodems-en-hoe-daar-mee-om-te-gaan			
Rijkswaterstaatskaart van door Rijkswaterstaat beheerde objecten ouder dan 1966 met een wettelijk beschermde hoge cultuurhistorische waarde, zie https://geoservices.rijkswaterstaat.nl/geoweb51/index.html?viewer=Monumenten.Monumenten	Proces	B-CW030	-
Werkveldspecifiek certificatieschema voor het systeemcertificaat Opsporen Conventionele Explosieven WSCS-OCE: 2012, versie 1	Proces	NE020	-
Rijkswaterstaat Brede Afspraak Duurzaam inkopen Versie 2.0, d.d. 27 september 2013	Proces	VW310	Q
CROW Publicatie 210, Richtlijn omgaan met vrijkomend asfalt, d.d. juni 2015 ISBN 978 90 6628 655 9 verkrijgbaar via CROW, zie www.crow.nl	Proces	B-UV340	-
Gedragscode soortenbescherming Rijkswaterstaat d.d. 11 augustus 2017, zie www.rws.nl/gedragscode-soortenbescherming	Proces	FF020	-
Kader Beheer Groenvoorzieningen 2013, zie http://www.rws.nl/groenvoorzieningen-infrastructuur	Proces	UT950	-
Richtlijnen voor inspectie en onderhoud van faunavoorzieningen bij Wegen 2008	Proces	FF050	X
Life Cycle Cost onderbouwing: LBT (LCC bij Beheer en Onderhoud Tool) en gestandaardiseerde business case template.	Proces	VI130 VI230 VW510	-
Veiligheidshandboek Rijkswaterstaat NEN 3140, zie http://publicaties.minienm.nl/documenten/veiligheidshandboek-nen-3140-rijkswaterstaat-zuid-holland-direct	Proces	VH060 VH070	-
BRL 5024 Beoordelingsrichtlijn voor het KOMO Procescertificaat voor het uitvoeren van bouwkundige vooropnamen, d.d. 3 oktober 2013 IKOB-BKB	Proces	BS100 BS150 BS160	-

Omschrijving referentie	**Vraagspecificatie deel**	**Eis / bepaling**	**Bijlage bij de Vraagspecificatie**
BRL 5023 Nationale beoordelingsrichtlijn voor het KOMO procescertificaat voor het proces van het meten van trillingen", d.d. 2 januari 2013 IKOB-BKB	Proces	BS210	-
Staat van prijzen per eenheid calamiteiten en incidenten	Basisovereenkomst Proces	Art.2 lid 8 B-US970 B-US990	R
Handreiking "Criteria voor toepassingen van bekledingen op waterkeringen", versie 0.4 d.d. 6 september 2010; los verstrekt	Eisen	AR.As.Re.DD.01	-
Eisen Bovenbouw v2; los verstrekt	Eisen	4.1	-
Eisen Markering v3; los verstrekt	Eisen	4.1	-
Componentspecificatie Openbare Verlichting v3.3; los verstrekt	Eisen	4.1	-
Eisen Voertuigkering v1.3.1; los verstrekt	Eisen	4.1	-
Eisen Berm v6; los verstrekt	Eisen	4.1	-
CROW Publicatie 207, Richtlijnen voor de bebakening en markering van wegen, d.d. 13 februari 2015 ISBN 9789066286429 verkrijgbaar via CROW, zie www.crow.nl	Eisen	4.2.2.2	-
CROW Publicatie 322, Richtlijnen Bewegwijzering 2014. d.d. 23 januari 2014 ISBN 9789066286313 verkrijgbaar via CROW, zie www.crow.nl	Eisen	4.2.4	-
Specificatie Functionele Inspecties en Testen, versie 2.4 d.d. 14-2-2019	Proces	US2400	AB
FIT_Typical, versie 4.1 d.d. 28-2-2019 (Generieke FIT-lijst)	Proces	US2400	AC
Specificatie NEN 3140 en NEN 3840 inspecties, versie 4.5 d.d. 18 januari 2019	Proces	VH081	AD
Productspecificaties Hydrografische opnemingen	Proces	US1240	-

Vertrouwelijkheid: RWS INFORMATIE

Bijlage A Informatie Areaal

A.1 Inleiding

Op de USB-stick / in de dataroom op TenderNed behorende bij de Overeenkomst zijn mappen aanwezig met de areaalgegevens. Het gaat hierbij om de kwantiteit (waaruit bestaat het Areaal) en de kwaliteit (toestandsinformatie en onderhoudshistorie) van het Areaal. Hieronder staat een toelichting per map. Sommige mappen bevatten de gegevens over het gehele Areaal of grote delen ervan, andere mappen bevatten submappen per beheerobject, bijvoorbeeld een sluis, brug of wegvak. Indien beschreven gegevens niet beschikbaar of niet van toepassing zijn, is dit expliciet aangegeven in de betreffende map.

A.2 Kwantitatieve beschrijving Areaal

A.2.1 GIS bestanden

Ordening: Areaalgeneriek
Inhoud: Kerngis Droog en/of Beheerkaart Nat shapefiles

- Geografische kaart van het Areaal uit het Geografische Informatie Systeem (GIS) van de Opdrachtgever te weten de beheerapplicatie Kerngis Droog en/of Beheerkaart Nat (zie document 'OMS, BMS en Beheerapplicaties'). Het GIS bestand geeft inzicht in onder andere Areaalgrenzen (eigendom, beheer, onderhoud), locatie beheerobjecten zoals gebouwen, terreinen, kunstwerken en locatie elementen zoals verlichtingsobjecten, geleiderail, bewegwijzering, DRIP's en TDI's. Verder de belangrijkste kenmerken van de areaaldelen, zoals soort areaal, nadere typering en specifieke kenmerken als archeologische, cultuurhistorische en/of landschappelijke waarde.
  Indien er areaaldelen ontbreken in de GIS bestanden, dan wil dit niet zeggen dat deze niet tot de scope behoren. De overige verstrekte informatie in deze bijlage A geeft hierover uitsluitsel.

Aandachtspunt:
De Opdrachtnemer kan de shapefiles *alleen* met behulp van CAD- of GIS-systemen raadplegen. Naar behoefte van de Opdrachtnemer kan het GIS bestand ook in de vorm van een Personal Geo-database worden geleverd, die echter *alleen* in te lezen is in de Rijkswaterstaatbeheerapplicatie Kerngis Droog c.q. Beheerkaart Nat, welke onder ArcGIS draait. De aan ArcGIS verbonden kosten zijn voor rekening van de Opdrachtnemer. De beide beheerapplicaties zijn te downloaden van www.rws.nl/datacontracteisen, tabblad 'Kerngis Droog respectievelijk Beheerkaart Nat'.
In bijlage A 2.1 is een ArcMap databasebestand meegegeven waarin de onderhoudsgrenzen zijn opgenomen. Tevens is in dit bestand inzichtelijk gemaakt welke andere beheerders aan het werkgebied grenzen.

A.2.2 Objectinformatie

Ordening: Areaalgeneriek
Inhoud:

- Rijkswaterstaat decompositie NEN-2767-4:
  Opbouw decompositie Rijkswaterstaat Areaal vanaf (delen van) rijkswegen c.q. rijkswateren tot op element- en/of bouwdeelniveau in een decompositierapportage uit het Rijkswaterstaat Infor EAM systeem.
  Zie bijlage A 2.2.1.
- Groenvoorziening en verhardingen (specificering).
  Zie BKN+.
  Cybersecurity weerstandsniveau beheerobjecten:

Een overzicht met het cybersecurity weerstandsniveau van de beheerobjecten, zoals kunstwerken, waarvoor dit van toepassing is.
Zie bijlage A 2.2.2.

- Materieel:
  Overzichten van en informatie over aggregaten, werktuigen etc.
  N.v.t.
- Areaaldelen met beperkte of geen gegevens:
  Overzicht van delen van het Areaal, waarvan nog geen of nog niet alle areaalgegevens zijn verwerkt in de beheerapplicaties, maar die wel binnen de scope vallen. Het gaat hierbij m.n. om areaalgegevens die van projecten moeten komen.
- Functionele inspecties en testen(FIT):
  Een overzicht van de beweegbare beheerobjecten waar FIT dienen te worden uitgevoerd.

Ordening: Objectspecifiek
Inhoud:

- Object infobladen, -paspoorten of -omschrijvingen:
  Informatie over en/of beschrijving van de functionele opbouw van objecten van bijvoorbeeld OV-installaties, VRI's en TDI's.
  Zie bijlage A 2.2.4.
- Overzichten installaties:
  Fabricaat, jaartal en typeaanduiding op elementniveau en afhankelijk van het niveau van onderhoud, risicoprofiel, functionaliteit en specialistisch werk aangevuld met primaire en secundaire bouwdelen.
  Eventueel aangevuld met een opsomming van calculeerbare eenheden als het aantal camera's en monitoren.
  Zie bijlage A 2.2.5
- Back-up proces:
  Niet meegeleverd ten behoeve van Taken en Services. Ter inzage op kantoor of op aanvraag.
- Overzichtstekening van complexen en andere objecten:
  Overzichtsinformatie hoe (grotere) beheerobjecten dan wel specifieke Areaaldelen zijn opgebouwd.
  Zie bijlage A 2.2.6
- Technische tekeningen en schema's:
  - *Niet* meegeleverd ten behoeve van Taken en Services. Ter inzage op kantoor.
  - Ten behoeve van Activiteiten: op hoofdlijnen t.b.v. vervanging of als uitgangspunt voor modificatie, alle aanvullende informatie is ter inzage op kantoor of op aanvraag.
- Cultuurhistorische waarden:
  Bouwhistorische onderzoeksrapporten van de door Rijkswaterstaat beheerde objecten ouder dan 1966 met een:
  1. wettelijk beschermde hoge cultuurhistorische waarde (rood genoteerd);
  2. niet wettelijk beschermde hoge cultuurhistorische waarde (oranje genoteerd).

  N.v.t.

A.2.3 Extra of uitgezonderd onderhoud

Ordening: Areaalgeneriek
Inhoud:

- Extra onderhoud:
  Aanvullende werkzaamheden buiten de scope of het Areaal.
  Zie bijlage A 2.3.3.
- Uitzonderingen / afbakeningen:
  Areaaldelen of werkzaamheden, die niet onder de scope vallen of informatie over tot waar de verplichting van de Opdrachtnemer loopt.

Vertrouwelijkheid: RWS INFORMATIE

Zie bijlage A 2.3.1.
- Afspraken derden:
  Afspraken, vastgelegd in overeenkomsten met en vergunningen van andere overheden, instanties of bedrijven voor bepaalde objecten over de Onderhoudswerkzaamheden.
  Zie bijlage A 2.3.2.

A.3 Beschrijving kwaliteit Areaal

A.3.1 Toestand Areaal

Ordening: Objectspecifiek
Inhoud:
- Toestandsrapportages:
  Het actuele beeld van de toestand van het Areaal.
  Zie bijlage A bijlage A 3.1.1.
- Specifieke toestandsrapportages:
  - Rapportage boomveiligheidscontrole:
    Meest recente versie VTA controle.
    Zie bijlage A 3.1.2. Het protocol is opgenomen in bijlage A 3.2.1.03.
  - Inventarisatieresultaten flora en fauna:
    Resultaten van de inventarisatie van aanwezige beschermde dieren en planten.
    Zie bijlage A 3.1.3.
  - Hydrografische werkzaamheden:
    N.v.t.
  - Onderwaterinspecties:
    N.v.t.
  - Asbestinventarisaties.
    Zie bijlage A 3.1.4.
- Ontbrekende toestandsinformatie:
  Inspecties conform de NEN-2767-4 van de onderdelen waarvan geen actueel beeld over de toestand van de betreffende onderdelen beschikbaar is.
  N.v.t.
- Rapportages Niet Gesprongen Conventionele Explosieven:
  Rapportages van vooronderzoeken met betrekking tot niet gesprongen conventionele explosieven.
  N.v.t.

A.3.2 Onderhoudsstrategie

Ordening: Areaalgeneriek
Inhoud:
- Onderhoudsregime groen:
  Onderhoudswerkzaamheden conform het geldende groenbeheerplan inclusief de bijbehorende beheertypen tekeningen en/of beheerbestanden.
  Zie bijlage A 3.2.1.03.
- Keuringsplichtige delen van objecten:
  Overzicht van specifieke keuringsplichtige objectdelen. Deze objectdelen zijn zoveel mogelijk in Infor EAM opgenomen met een kopie van het certificaat (origineel bij het objectdeel zelf). Alle overige middelen zijn verantwoordelijkheid van de Opdrachtnemer zelf. Het gaat hierbij om objectdelen met wettelijke keuringen zoals hijs-, hef-, hulp- en veiligheidsmiddelen en speeltoestellen, roldeuren en intercominstallaties.
  Zie ook bijlage A 2.2.5.
- Waterbodem:
  Nautisch profiel per beheerobject (sluis, rivier/kanaalvak, meer, etc.).
  N.v.t.
- Waterniveau:
  Streefpeil, maximum- & minimumpeil.

N.v.t.

Ordening: Objectspecifiek
Inhoud:

- Onderhoudsconcept, aan de hand waarvan Opdrachtnemer het Onderhoudsregime dient te bepalen. Zie bijlage A 3.2.1.
- Onderhoudsregime installaties:
  Huidige onderhoudsinterventies of onderhoudsmethodieken.
  Zie Infor EAM. Deze informatie in Infor EAM is slechts informatief, er kunnen geen rechten aan deze informatie ontleend worden.
- Onderhoudsregime civiele constructies die van invloed zijn op de primaire beschikbaarheid van beweegbare objecten:
  Zie Infor EAM. Deze informatie in Infor EAM is slechts informatief, er kunnen geen rechten aan deze informatie ontleend worden.
  Huidige onderhoudsinterventies of onderhoudsmethodieken.
  Zie Infor EAM. Deze informatie in Infor EAM is slechts informatief, er kunnen geen rechten aan deze informatie ontleend worden.
- Onderhoudshandboeken:
  Ter inzage op kantoor/object, tenzij specifiek voorgeschreven.
  Zie bijlage A 3.2.1.1.1.
- Draaiboeken:
  Ter inzage op kantoor/object, tenzij specifiek voorgeschreven.
- Overzicht kritieke reserveonderdelen (consumables, Wisseldelen en Hulpmiddelen (onderhoudsvoorzieningen)):
  Zie bijlage A 3.2.3.
- Garantieverplichtingen (Garantiebank Verhardingen):
  Afspraken of termijnen die de Opdrachtnemer moet bewaken.
  Uitgezonderd hierop zijn de garanties, die verstrekt zijn voor asfaltverhardingen. Deze asfaltgaranties zijn opgenomen in de Garantiebank van Rijkswaterstaat, waarvoor de Opdrachtnemer toegang krijgt conform bijlage B "Levering areaalgegevens" bij de Vraagspecificatie, § B.2.1 'Toegang tot beheerapplicaties'.
  Zie bijlage 3.2.4.

A.3.3 Specifieke eisen

Ordening: Objectspecifiek

- Geplande en ongeplande niet-beschikbaarheid van beheerobjecten of groepen van beheerobjecten, die dienen te blijven binnen de grenzen die voor deze beheerobjecten of groepen van beheerobjecten zijn opgenomen.
  Zie hiertoe bijgevoegde hoofdstukken 3 uit de prestatiegestuurde instandhoudingsplannen (P-IHP's).

A.3.4 Historische onderhoudsgegevens

Ordening: Areaalgeneriek
Inhoud:

- Calamiteitenregister:
  Globaal overzicht calamiteiten en schades van de afgelopen jaren.
  Zie Infor EAM.
- Historische overzichten afgevoerd materiaal:
  Uit OMS van de vorige opdrachtnemer op basis van afleverbonnen.
  Zie bijlage A 3.4.1.
- Historische overzichten verbruiksmaterialen:
  Uit OMS van de vorige opdrachtnemer of opdrachtbonnen Rijkswaterstaat.
  Zie bijlage A 3.4.2.

Ordening: Objectspecifiek
Inhoud:

Vertrouwelijkheid: RWS INFORMATIE

- Historisch overzicht storingen en gebreken:
  Storingen-/gebrekenregisters.
  Zie Infor EAM.
  Analyses 3-5 jaar ingedeeld in storing, oorzaak, reparatie en actie.
  Zie Infor EAM.

A.3.5 *Risicodossier*

Ordening: Areaalgeneriek

Inhoud:

- Rijkswaterstaat areaalrisico's:
  Areaalspecifieke technische risico's, die de Opdrachtnemer *niet* vanuit zijn vakkennis kan weten.
  Zie Bijlage A 3.2.1 "Onderhoudsconcept".
- Integraal veiligheidsdossier:
  V&G dossier met generieke en projectspecifieke V&G risico's, RI&E's. Zie separate documenten in bijlage A 3.5.1.
  Het Integraal Veiligheidsplan is opgenomen in bijlage K "Integraal Veiligheidsplan" bij de Vraagspecificatie.
- Rijkswaterstaat onderhoudsplan:
  RUPS programmering met de al geïdentificeerde onderhoudsrisico's met bijbehorende maatregelen, zo mogelijk nader toegelicht met onderliggende rapportages.
  Zie de toestandsrapportages in bijlage A 3.1.1. "Conditie en interventiemomenten".

Bijlage B Levering areaalgegevens

B.1 Algemeen

In deze bijlage staan de eisen met betrekking tot de levering van areaalgegevens ten behoeve van het beheer van het Areaal door Rijkswaterstaat.

B.1.1 Wijziging specificaties en software

Tijdens de looptijd van de Overeenkomst kunnen de specificaties van de geo- en databestanden genoemd in deze bijlage wijzigen. De Opdrachtnemer dient te borgen, dat het door hem op te leveren bestand conform de op het moment van levering geldende versie is opgebouwd. De Opdrachtnemer kan er vanuit gaan, dat deze wijzigingen minimale extra kosten met zich meebrengen. Indien de wijzigingen meer kosten dan wat redelijkerwijze door de Opdrachtnemer kan worden ingeschat, dient hij dit onderbouwd aan de Opdrachtgever voor te leggen.

Voor de in deze bijlage genoemde software en beheerapplicaties geldt, dat ten tijde van de oplevering, de dan bij de Opdrachtgever vigerende versie dient te worden gehanteerd.

B.2 Beheerapplicaties

B.2.1 Toegang tot beheerapplicaties

De Opdrachtgever verleent de Opdrachtnemer toegang tot de nodige beheerapplicaties van de Opdrachtgever. Voor de toegang tot de beheerapplicaties bestaan verschillende procedures. Het is belangrijk om in eerste instantie toegang te vragen voor de medewerkers van de Opdrachtnemer die daadwerkelijk areaalgegevens, bijvoorbeeld bij storingen, in het BMS gaan bewerken. Naderhand kan altijd voor andere medewerkers, eventueel met andere taken, toegang worden aangevraagd. Een account mag alleen worden gebruikt door degene voor wie het is aangevraagd. Tevens stelt de Opdrachtgever, indien nodig, één PC met benodigde software beschikbaar op Rijkswaterstaatlocatie.

De aanvraag voor de toegang tot beheerapplicaties gaat als volgt:

- DISK en DTB: de Opdrachtnemer kan de toegang tot DISK en DTB niet zelf aanvragen. Op verzoek van de Opdrachtnemer zal de Opdrachtgever de aanvraag voor netwerktoegang derden RWS indienen.;
- Infor EAM; toegang vragen via OG. Er zijn 6 desktop licenties en 10 mobile acces licenties beschikbaar voor de Opdrachtnemer.
- Overige beheerapplicaties: op verzoek van de Opdrachtnemer zal de Opdrachtgever hiervoor de contactpersoon doorgeven.

Het BMS bestaat uit de volgende beheerapplicaties:

Beheerapplicatie	**Van toepassing**	**Toegang**
Infor EAM	Ja	Internet
Digitaal Topografisch Bestand (DTB)	Ja	Internet
Kerngis droog	Ja	PC district
Beheerkaart Nat Plus	Ja	PC district
Garantiebank verhardingen	Nee	PC district
DISK	Ja	Internet
ARA-PRO/ALERT (storingsmeldsysteem)	Ja	PC district
TMX (storingen van pompen en verkeersregelinstallaties)	Nee	PC district
MobiMaestro	Nee	PC district
Aquaview	Nee	PC district

Vertrouwelijkheid: RWS INFORMATIE

RCM Cost	Nee	PC district
EOD verkenner	Nee	PC district
Meridian	Ja	PC district

B.2.2 *Consistentie tussen beheerapplicaties*

Rijkswaterstaat heeft een aantal beheerapplicaties, met daarin gedeeltelijk dezelfde areaalobjecten, alleen ieder met een eigen doel en inhoud (document 'OMS, BMS en Beheerapplicaties' te downloaden van www.rws.nl/datacontracteisen), maar waarvan de inhoud wel aan elkaar is gerelateerd.

De Opdrachtnemer dient bij het actualiseren van areaalgegevens de consistentie tussen de verschillende beheerapplicaties te borgen, zodanig dat na de Werkzaamheden de meervoudig opgeslagen areaalgegevens, met name decompositie en beschrijvende kenmerken, in de beheerapplicaties consistent ten opzichte van elkaar blijven. Dit geldt met name bij nieuwe situaties, omdat dan oude areaaldelen uit de bestanden verdwijnen c.q. op vervallen komen te staan en nieuw areaal wordt geregistreerd. Bij 1-op-1 vervangingen van areaaldelen, zoals bij onderhoud veelal het geval is, zal in de decompositie niet zoveel wijzigen en kan het muteren naast elkaar lopen. Zeker de mutaties van de GIS beheerapplicaties en DISK/Infor-EAM RWS kunnen vaak parallel lopen.

De Opdrachtnemer dient minimaal te voldoen aan de volgende eisen met betrekking tot het borgen van de consistentie van de areaalgegevens en de volgorde van het actualiseren van de beheerapplicaties:

1. De Opdrachtnemer dient, voordat de beheerapplicaties worden aangepast, met de Opdrachtgever een datum af te spreken waarop de wijzigingen plaatsvinden.
2. DISK/Infor EAM (kunstwerken):
   a. Nieuwe kunstwerken of onderdelen aanleveren voor Infor EAM.
   b. De decompositie van kunstwerken conform het Infor EAM aanleveren voor DISK.
3. GIS bestanden:
   a. Eerst het Digitaal Topografisch Bestand (DTB) actualiseren, omdat dit het leidende systeem voor wat betreft topografie is.
   b. Daarna met behulp van het nieuwe DTB het Kerngis Droog respectievelijk Beheerkaart Nat Plus(BKN+) opbouwen en aanvullen met administratieve gegevens, onder andere bij kunstwerken de beheercode en relevante kenmerken uit DISK.
   c. De volgende twee GIS-lagen/beheerapplicaties dienen na de bijwerking van Kerngis Droog / Beheerkaart Nat te worden bijgewerkt:
      i. Kabels &Leidingen GIS-laag in Kerngis;
      ii. Garantiebank Verhardingen (overige garanties in Ultimo RWS).
4. Infor EAM:
   a. De decompositie van het niet-kunstwerken Areaal in overeenstemming met BKN+ en Kerngis droog aanleveren voor Infor EAM.
5. Meridian:
   De decompositie ten behoeve van Meridian in overleg met OG bijwerken.

B.2.3 *Inrichting Infor EAM*

- De Opdrachtgever heeft als CMMS - onderdeel (Computerized Maintenance Management System) van haar BMS de beheerapplicatie Infor EAM dat via internet te benaderen is. De Opdrachtnemer dient het infor EAM systeem ook te gebruiken als zijn OMS (eis CM020).
- De inrichting van het Infor EAM systeem wordt door Opdrachtgever gedaan op basis van het datamodel en door de Opdrachtnemer aangedragen benodigde processen.

- Aanpassing beheerapplicatie Infor EAM: De Opdrachtgever behoudt zich het recht voor om binnen de contractperiode het datamodel aan te passen dan wel een CMMS-beheerapplicatie van een andere fabrikant te gaan gebruiken. Opdrachtnemer zal hieraan haar medewerking verlenen. Daar waar in het contract Infor EAM staat dient in dat geval de naam van de nieuwe CMMS-beheerapplicatie te worden gelezen.

B.3 Beheer en Onderhoud Managementgegevens

B.3.1 Decompositie (objectenboom)

De Opdrachtnemer dient een voorstel voor de nieuwe of gewijzigde decompositie in de beheerapplicaties van het Beheer Management Systeem aan te leveren en bij het actualiseren gebruik te maken van de NEN 2767 decompositie en de aanvullende Rijkswaterstaatspecificatie 'Decompositiekader NEN 2767 RWS'. Dit document is te downloaden van www.rws.nl/datacontracteisen, tabblad "Ultimo".

De Opdrachtnemer dient er rekening mee te houden, dat pas na verwerking van de nieuwe of gewijzigde decompositie door de Opdrachtgever de bijbehorende gegevens door de Opdrachtnemer in Infor EAM en Meridian kunnen worden opgenomen. De Opdrachtgever heeft twee weken nodig om de nieuwe of gewijzigde decompositiegegevens te verwerken. De Opdrachtnemer dient in overleg met de Opdrachtgever hierover afspraken te maken.
De Opdrachtnemer dient in overleg met de Opdrachtgever de nieuwe of gewijzigde decompositie vooruitlopend op het af- of opleverdossier, zo nodig, in delen leveren.

De Opdrachtnemer dient er rekening mee te houden, dat de NEN 2767 en de aanvullende Rijkswaterstaatspecificatie nog veranderen, waardoor mogelijk de decompositie in het Beheer Management Systeem wijzigt en de Opdrachtnemer de decompositie in zijn Onderhoud Management Systeem eveneens dient te wijzigen.

B.3.2 Actueel houden Infor EAM van Opdrachtgever

De Opdrachtnemer dient in de beheerapplicatie Infor EAM de kwalitatieve gegevens te actualiseren conform de feitelijke toestand van het Areaal en de kwantitatieve gegevens te actualiseren, die als gevolg van de Werkzaamheden wijzigen.
Het invoeren en vastleggen in het Infor EAM van de Opdrachtgever dient binnen één week na afronding van de betreffende Werkzaamheden te gebeuren, tenzij bij de betreffende eis in de Vraagspecificatie een andere periode is aangegeven.
Het invoeren dient te gebeuren conform de volgende specificaties:

- Datamodel Infor EAM
- Handleiding Infor EAM

B.3.3 Meridian

De Opdrachtnemer dient na de Werkzaamheden de brondocumenten in de beheerapplicatie Meridian te actualiseren dan wel nieuwe documenten te maken en deze te leveren aan de Opdrachtgever ten behoeve van opname in Meridian. Tevens dient de Opdrachtnemer de meta-data van deze (bron)documenten te leveren aan de Opdrachtgever. De Opdrachtnemer dient aan te geven welke (bron)documenten vervallen inclusief de vervaldatum en vervalreden.
De Opdrachtnemer dient ten behoeve van het actualiseren de brondocumenten op te vragen bij de Opdrachtgever. De Opdrachtnemer dient ten behoeve van nieuwe documenten een documentnummer aan te vragen bij de Opdrachtgever.
Het opvragen, leveren en actualiseren dient te gebeuren conform de volgende specificatie:

- Eisen voor Datamodel Technische Documentatie.

Dit document is te downloaden van www.rws.nl/datacontracteisen, tabblad "Meridian".

Vertrouwelijkheid: RWS INFORMATIE

B.4 Areaalgegevens

B.4.1 Areaalgegevens

De Opdrachtnemer dient de areaalgegevens van de door hem uitgevoerde Werkzaamheden te leveren, zodat Rijkswaterstaat een goed beheer over het Areaal kan doen. Hiervoor dient de Opdrachtnemer de volgende lijst als uitgangspunt te gebruiken:

- Gegevensmatrix Areaal Nat

Opdrachtnemer dient bij het bijhouden van het BMS de werkwijze zoals beschreven in "Invulinstructie BMS Zee & Delta nat 25 3 2019.doc" te gebruiken.

Indien er areaalgegevens zijn, die niet op de lijst staan, maar die naar analogie van de rest van de lijst logischerwijs ook zouden moeten worden geleverd, dient de Opdrachtnemer hiervoor zo spoedig mogelijk na constatering een voorstel aan de Opdrachtgever te doen en deze na goedkeuring van het voorstel te leveren.
Indien door de Opdrachtnemer te bouwen objecten ontbreken op de lijst, dan dient hij zo spoedig mogelijk na constatering een voorstel te doen aan de Opdrachtgever over welke areaalgegevens van het object logischerwijs conform vergelijkbare objecten op de lijst door hem aan de Opdrachtgever moeten worden geleverd. Tevens dient de Opdrachtnemer deze areaalgegevens te leveren na goedkeuring van het voorstel door de Opdrachtgever.

De wijze waarop de gegevens moeten worden aangeleverd is afhankelijk van het systeem respectievelijk het format, dat in de bovengenoemde lijst per gegeven staat aangegeven in de kolom 'Opslagsystemen / Format voor gegeven'. Indien er meerdere systemen en/of formats staan genoemd, dient voor al deze systemen en formats in het eigen formaat gegevens te worden aangeleverd.
Bestanden dienen een naamgeving te hebben conform de aan het bestand gerelateerde documentatie. Indien dit niet beschreven is, dient de bestandsnaam de inhoud van het bestand weer te geven door middel van de typering van het document en een kenmerk (bijvoorbeeld het woord vergunning met vergunning nummer).

<u>Waterareaal</u>

- ArcGIS: in shapefiles opgebouwd conform regionale indeling;
- AutoCad: conform paragraaf "AutoCad bestanden en tekeningen";
- BKN+: conform invulinstructie BKN+;
- Gegevensdrager: ieder softwarepakket dient op een aparte gegevensdrager te worden geleverd, waarop tevens een bestand staat met een beschrijving van de inhoud van/bestanden op de gegevensdrager;
- DISK c.q. Kunstwerkpaspoort: indien Activiteiten met betrekking tot kunstwerken plaatsvinden, zijn dan wel worden de eisen nader gespecificeerd in aanvullende activiteitenspecificaties;
- Document: opzet conform voorschriften regionaal onderdeel. In geval een specifiek voorschrift wordt genoemd, geldt het genoemde voorschrift;
  bestandsformaat inleesbaar in MS Office Professional Plus 2010;
  indien alleen analoog beschikbaar: OCR (Optical Caracter Regognition) scannen en aanleveren in pdf a-1a ;
- DMS (Document Management Systeem): aanleveren ten behoeve van Hummingbird;
- IENC (Inland Electronic Navigation Chart): hiervoor <u>geen</u> gegevens aanleveren. De benodigde gegevens worden door Rijkswaterstaat uit andere beheerapplicaties gegenereerd.
- DTB (voorheen IVRI): conform paragraaf "Digitaal Topografisch Bestand";
- IVS: volgens regionale specificaties;
- Kerngis: conform paragraaf "Kerngis";
- KLIC: conform regelgeving van het Kadaster / KLIC (WION);
- Log-apparaat: uitdraai uit apparaat;
- Munice (Kadaster): hiervoor geen gegevens aanleveren. De benodigde gegevens worden via een ander Rijkswaterstaatproces verzameld;

-
- TDMS (Technisch Document Management Systeem): volgens regionale specificaties;
- VAMIS: volgens regionale specificaties.
- Wab*info: conform Vraagspecificatie Proces, §5.4.13, eis US1640;
- TCD (Technisch Constructie Dossier): volgens regionale specificaties;
- Infor EAM; volgens regionale specificaties;

B.4.2 AutoCad bestanden en tekeningen

De Opdrachtnemer dient de as-built bestanden en tekeningen betreffende de bestaande situatie op te vragen bij de Opdrachtgever.
De Opdrachtgever levert deze documenten aan inclusief een registratielijst (importblad Meridian, zie bijlage 4.2).
In de tekeningenlijst bij deze bijlage is per tekening de vorm aangegeven waarnaar de betreffende tekening moet worden aangepast. Tekeningen waar is aangegeven 'vervangen door een DWG volgens NLCS/TOLGI/tekeningenrichtlijn' dienen te worden aangeleverd in de gevraagde vorm.

Voor alle aangepaste of nieuw gerealiseerde (civiele) Werken dienen de as-built bestanden en tekeningen geometrisch en inhoudelijk een exacte weergave te zijn van het gerealiseerde Werk. Tevens dienen de vervallen en aangepaste as-built bestanden en tekeningen als gevolg van het gerealiseerde Werk aan de Opdrachtgever te worden gerapporteerd.

De Opdrachtnemer dient de as-built bestanden en tekeningen te leveren conform de volgende specificaties:

- Bestandsformaat: inleesbaar in Autocad Map 3D 2017;
- Tekeningenformaat: opgebouwd conform NLCS (Nederlandse CAD standaard). Voor nadere informatie zie: www.nlcs-gww.nl
- Document "Aanvullende eisen tekenwerk Rijkswaterstaat, versie 1.0" te downloaden van www.rws.nl/datacontracteisen, tabblad CAD-bestanden en –tekeningen Rijkswaterstaat.
- Document "Tekenvoorschriften object- en lijninfrastructuur gebonden installaties" te downloaden van www.rws.nl/datacontracteisen, tabblad CAD-bestanden en –tekeningen Rijkswaterstaat.
  Met in aanvulling op hoofdstuk 7 document "Tekenvoorschrift werktuigbouw Regio Zeeland v0.2".
  Zie bijlage B 4.
- De registratielijst (importblad Meridian) dient bijgewerkt te worden met de meta-informatie van alle geleverde As-built bestanden, tekeningen en documenten.
- De Opdrachtnemer dient de aangevraagde documenten binnen zes weken na uitgifte te retourneren.
- Voor nieuwe tekeningen/documenten dienen registratienummers aangevraagd te worden bij de Opdrachtgever.
- Overige documenten: (niet zijnde tekeningen) volgens PDF/A-1b standaard.
- De Opdrachtnemer dient een lijst aan te leveren met alle bestaande tekeningen en documenten die, vanwege het werk, kunnen vervallen.

Roodrevisies

De Opdrachtnemer dient bij wijzigingen van het areaal en van installaties in het areaal, de betreffende tekeningen en/of documentatie van het areaal of de installaties in het areaal direct aan te passen middels roodrevisie. Aangegeven dient te worden wie de aanpassing heeft gedaan, wanneer en met welke reden. De roodrevisie dient gedetailleerd, duidelijk leesbaar, betrouwbaar en compleet te zijn en heeft een tijdelijk karakter. De Opdrachtnemer dient uiterlijk 15 dagen na voltooiing van de Werkzaamheden op basis van de roodrevisie de bestaande tekeningen as-built te maken. Indien de roodrevisie van invloed is op andere tekeningen en/of documentatie dienen ook deze aangepast te worden.

Vertrouwelijkheid: RWS INFORMATIE

B.4.3 *Digitaal Topografisch Bestand*

De Opdrachtnemer dient de gewijzigde terreinsituatie digitaal en geïntegreerd in het beschikbaar gestelde Digitaal Topografisch Bestand (DTB) te leveren conform de volgende specificaties:

- Productspecificaties Digitaal Topografisch Bestand;
- Handboek DTB-Droog en DTB-Nat.

Alle in het kader van het Werk nieuw aangebrachte en gewijzigde topografie dient te worden ingewonnen. Onder gewijzigde topografie worden ook vlakken en lijnen verstaan die door vergroten, verkleinen of verleggen van aangrenzende vlakken respectievelijk lijnen kleiner of groter zijn geworden.
Deze documenten zijn te downloaden van www.rws.nl/datacontracteisen, tabblad "Digitaal Topografisch Bestand".

B.4.4 *Kerngis*

Indien Werkzaamheden aan rijkswegen dan wel kabels & leidingen zijn verricht, dient de Opdrachtnemer alle benodigde gegevens in het kader van het Werk ten behoeve van het Kerngis te leveren conform de volgende specificaties:

- Productspecificatie Kerngis-data;
- Invulinstructie datamodel Kerngis 2007.

Deze documenten zijn te downloaden van www.rws.nl/datacontracteisen, tabblad "Kerngis Droog en Beheerkaart Nat".
Het bijwerken van de Kerngis-database vindt plaats op kantoor van het betreffende district met behulp van IT-voorzieningen van de Opdrachtgever.
Levering van Kerngis bestanden dient altijd tegelijk met de levering van bijbehorende DTB bestanden te gebeuren omdat de topografie in Kerngis op DTB is gebaseerd.

Kabel & Leiding informatie vanwege de WIBON dient tijdig, conform VSP 4.2.3 "Gegevens verstrekken Kabels en Leidingen Rijkswaterstaat", geleverd te worden volgens het datamodel voor Kabels en Leidingen van Kerngis.
De Opdrachtgever stelt de 'Controletool Kerngis-data' beschikbaar, die voor de Opdrachtnemer een hulpmiddel kan zijn om de kans op tekortkomingen in de door de Opdrachtnemer te leveren Kerngis-data te verkleinen. Deze "Controletool Kerngis-data" is in beheer bij Rijkswaterstaat CIV en is te downloaden van www.rws.nl/datacontracteisen, tabblad "Kerngis Droog en Beheerkaart Nat". Voor het gebruik van de "Controletool Kerngis-data" geldt de meegeleverde disclaimer.

B.4.5 *Beheerkaart Nat Plus*

Indien Werkzaamheden aan rijksvaarwegen zijn verricht, dient de Opdrachtnemer alle benodigde gegevens in het kader van het Werk ten behoeve van de Beheerkaart Nat te leveren conform de volgende specificaties:

- Productspecificatie Beheerkaart Nat 3 (BKN3);
- Invulinstructie Beheerkaart Nat 3 (BKN3).
- Productspecificatie Beheerkaart Nat Plus, op te vragen bij Opdrachtgever;
- Invulinstructie Beheerkaart Nat Plus, op te vragen bij Opdrachtgever.

Levering van Beheerkaart Nat en Beheerkaart Nat Plus bestanden dienen altijd tegelijk of na de levering van bijbehorende DTB bestanden te gebeuren omdat de topografie in Beheerkaart Nat op DTB is gebaseerd.
Deze documenten zijn te downloaden van www.rws.nl/datacontracteisen, tabblad "Kerngis Droog en Beheerkaart Nat".

B.4.6 *Wijzigingen objectinformatie*

De Opdrachtnemer dient wijzigingen aan objecten door te voeren op de desbetreffende objectinfobladen en/of informatieoverzichten, zoals verstrekt in bijlage A 2.2.4.

B.4.7 *Doorrijprofielen*

N.v.t.

B.4.8 Garantiebank

N.v.t.

B.4.9 Hydrografische Werkzaamheden

Geo-referentie

Het te gebruiken coördinatenstelsel in de Overeenkomst is:

- RD-NAP conform de meest recente versie van de procedure RDNAPTRANS™. Informatie over deze procedure is te vinden op https://zakelijk.kadaster.nl/transformatie-van-coordinaten
- ETRS89 UTM zone 31N voor het horizontale vlak en LAT voor het verticale vlak.

Indien gewerkt wordt met profielgegevens dient de Opdrachtnemer voor de uitvoering van de Werkzaamheden, in overleg met de Opdrachtgever, een kilometrering en een aslijn vast te stellen.
De volgende kenmerken dienen te worden vastgesteld:

- ligging van de aslijn (XY-coördinatenlijst);
- richting van de oplopende kilometrering;
- definitie van het nulpunt (XY-coördinaten van een bepaalde kilometerwaarde).

Alle voor de Overeenkomst gebruikte grids dienen te voldoen aan het volgende:

- de oriëntatie van de gridcellen is noord gericht;
- de virtuele oorsprong (0,0) van het XY-coördinatenstelsel valt samen met een hoekpunt van een gridcel.

Kwaliteit van hydrografische opnemingen

Op de door de Opdrachtnemer uit te voeren hydrografische opnemingen zijn de "Nederlandse normen voor hydrografische opnemingen" van toepassing. Deze normen zijn te downloaden van: www.rws.nl/datacontracteisen, tabblad Hydrografische normen.
In het kader van deze normen dient de Opdrachtnemer te voldoen aan Norm A, met uitzondering van de eisen over een volledig bodemonderzoek.
Voor de horizontale component zijn de eisen strenger dan de aangegeven hydrografische norm. Hiervoor dient voldaan te worden aan een 95% betrouwbaarheidsniveau van 0,35 m. + 1% van de diepte.
Voor de verticale component zijn de eisen strenger dan de aangegeven hydrografische norm. Hiervoor gelden voor het 95% betrouwbaarheidsniveau de parameterwaarden a = 0,10 m en b = 0,0075.
Het totaal van de eventueel nog aanwezige restfouten van gecorrigeerde systematische fouten mag maximaal 5 cm bedragen.

De Opdrachtnemer dient de hydrografische opnemingen uit te voeren als gebiedsdekkende metingen. Hierbij dient de datadichtheid (na validatie) minimaal te voldoen aan de volgende eisen:

- 10 hits per gridcel (moet gelden voor 95% van de gridcellen), uitgaande van een grid met gridcellen van 1x1 m; de gebieden (max. 5%) met minder dan het in het vorige punt genoemde aantal hits per gridcel mogen aaneengesloten niet groter zijn dan 100 m²;

Voor gebieden met een diepte van meer dan 10 meter kan in overleg met de Opdrachtgever worden afgeweken van de hier gestelde eis aan de datadichtheid.
De Opdrachtnemer dient de hydrografische opnemingen uit te voeren volgens een raaienpatroon. Hierbij dient de datadichtheid (na validatie) te voldoen aan de volgende eis:
1 dwarsraai per 25 m en 1 meetpunt per meter voor 95% van de raai.
De maximale afwijking uit de raai mag niet meer bedragen dan 10 m.

Daar waar de hydrografische opnemingen gecorrigeerd moeten worden voor de ter plaatse geldende waterstand, dient de Opdrachtnemer de manier waarop dit gebeurt

Vertrouwelijkheid: RWS INFORMATIE

te bepalen in overleg met de Opdrachtgever.Bij de hydrografische opnemingen dient de Opdrachtnemer een frequentie te gebruiken van minimaal 200 kHz.

B.4.10 *Nationaal wegenbestand (NWB) en WEGGEGevens (WEGGEG)*
De Opdrachtnemer dient de NWB-gegevens aan de Opdrachtgever te leveren conform de Aanleverspecificaties NWB en WEGEG.
Deze specificaties zijn te downloaden van www.rws.nl/datacontracteisen, tabblad "Nationaal Wegenbestand".

De Opdrachtnemer dient de data van het ontwerp van tijdelijke en definitieve situaties, uiterlijk 6 weken voor de openstelling van de wegsituatie, te leveren conform de aanleverspecificaties NWB en WEGGEG.

B.4.11 *Electronische Navigatiekaart (ENC)*
De Opdrachtnemer dient in het kader van aanpassingen aan, op of in het water(weg)infrasysteem de data conform de "featurelijst voor enc.xlsx" 10 dagen voordat de aanpassing wordt gerealiseerd te leveren door middel van een ontwerptekening. De ontwerp-tekening dient inleesbaar te zijn in ArcGIS of Autocad.
De featurelijst is te downloaden van www.rws.nl/datacontracteisen, tabblad "Electronische navigatiekaart (ENC)".

De Opdrachtnemer dient de data van het ontwerp van tijdelijke en definitieve aanpassingen in, aan of op de vaarweg die minimaal een maand van kracht zijn, uiterlijk 10 dagen voor de aanpassing wordt gerealiseerd, te leveren.

Bijlage C Calamiteiten, incidenten en schadeherstel

Deze bijlage beschrijft de eisen aan voorkomende Werkzaamheden (Taken, Services en/of Activiteiten) en het Areaal waaraan de Opdrachtnemer dient te voldoen bij het verrichten van Werkzaamheden bij calamiteiten en incidenten in het Areaal.

C.1 Algemeen

1. De Opdrachtnemer draagt zorg voor het veilig en deugdelijk uitvoeren van de Werkzaamheden, conform de daarvoor geldende wet en regelgeving, alsook het veilig en deugdelijk opheffen van de ingestelde maatregelen.

2. De Opdrachtnemer draagt zorg voor de beschikbaarheid van (hulp)materieel, gereedschap en materiaal dat noodzakelijk kan zijn voor de Werkzaamheden.

3. De Opdrachtnemer verzorgt veilige en goede verkeersmaatregelen conform het bepaalde in de Overeenkomst, inclusief het daarvoor benodigde materieel, materiaal en personeel. Het betreft zowel stationaire als rijdende verkeersmaatregelen.

C.2 Voorkomende werkzaamheden bij veiligstellen en beschikbaar stellen

C.2.1 Voorkomende werkzaamheden tijdens calamiteit en/of incident

1. De Opdrachtnemer verwijdert zaken als afgevallen lading, puin, levende en/of gewonde dieren en kadavers, brokstukken, afval, zand, vloeibare substanties en andere ongewenste materialen en vaste en vloeibare stoffen van en uit het wegdek en berm, ongeacht de vorm of omvang. Voor de afgevallen lading geldt dat de calamiteitengemachtigde bepaalt waarheen die moet worden afgevoerd.

2. De Opdrachtnemer verricht noodreparaties en/of voert noodhandelingen uit aan de weg, beschadigd wegmeubilair en kunstwerken om ervoor te zorgen dat het wegverkeer zo snel mogelijk veilig hervat kan worden.
   Beschadigd wegmeubilair bestaat voornamelijk uit bermbeveiliging en openbare verlichting. De calamiteitengemachtigde bepaalt of de schade door de Opdrachtnemer hersteld dient te worden.

3. De Opdrachtnemer graaft (verontreinigde) grond af en voert deze af volgens de geldende voorschriften. De Opdrachtnemer herstelt de berm naar de oorspronkelijke staat.

C.2.2 Voorkomende Werkzaamheden aangaande verkeer

1. De Opdrachtnemer plaatst het door hem ter beschikking te stellen calamiteitenscherm op aangeven van de calamiteitengemachtigde om kijkfiles te voorkomen. De Opdrachtnemer verwijdert het calamiteitenscherm op aangeven van de calamiteitengemachtigde.

C.2.3 Voorkomende Werkzaamheden aangaande milieu

1. Indien de Opdrachtnemer oppervlaktewater-, bodem- en/of grondwaterverontreiniging constateert tijdens een calamiteit en/of incident, dan adviseert de Op-

Vertrouwelijkheid: RWS INFORMATIE

drachtgever over een efficiënte aanpak met betrekking tot het inperken van de verontreiniging en het terstond opruimen. De Opdrachtnemer neemt de noodzakelijke bodem- en watermonsters conform de daarvoor geldende wet- en regelgeving om de effectiviteit van de sanering te kunnen bepalen evenals een referentiemonster om de natuurlijke achtergrondwaarde te bepalen. De Opdrachtnemer draagt zorg voor de sanering.

2. De Opdrachtnemer treft maatregelen om uitbreiding van de milieuvervuiling te voorkomen dan wel te beperken en ruimt de milieuvervuiling op conform de daarvoor geldende wet- en regelgeving.

C.2.4 Voorkomende Werkzaamheden aangaande gevaarlijke stoffen

1. De Opdrachtnemer verricht de dienstverlening ten aanzien van gevaarlijke stoffen in overleg met brandweer en de calamiteitengemachtigde. De Werkzaamheden mogen alleen verricht worden in overleg met de brandweer indien aanwezig. De Opdrachtnemer adviseert de calamiteitengemachtigde en de aanwezige brandweer over de te volgen werkwijze en ondersteunt de brandweer bij haar werkzaamheden in overleg met de calamiteitengemachtigde.

2. De Opdrachtnemer stelt binnen de daarvoor vastgestelde responstijd na vaststelling van de betrokken chemische en/of gevaarlijke stof de benodigde stoffen, materialen en materieel beschikbaar om de gevaarzetting te neutraliseren of te beperken.

3. De Opdrachtnemer verpakt vrijgekomen gevaarlijke (afval)stoffen en voert deze af conform de daarvoor geldende wet- en regelgeving op een veilige en verantwoorde wijze. Hiertoe behoort ook het eventueel overpompen van vloeibare (gevaarlijke) stoffen. De Opdrachtnemer levert het benodigde (verpakkings)materiaal en stelt benodigd materieel en personeel ter beschikking.

C.2.5 Voorkomende Werkzaamheden aangaande afvoer van materiaal en stoffen, niet zijnde gevaarlijke stoffen

1. De Opdrachtnemer laadt vrijgekomen goederen, materialen, afvalstoffen en andere vaste en vloeibare stoffen op of over in opdracht van de Rijkswaterstaat calamiteitengemachtigde en in overleg met de gecontracteerde IM-berger en verplaatst deze goederen naar een afgesproken bestemming.

C.2.6 Materieel en uitrusting

1. De Opdrachtnemer heeft ter plaatse van de afhandeling te allen tijde beschikking over:
   - vijftien verkeerskegels;
   - materiaal om vloeistoffen mee op te vangen;
   - absorptiekorrels;
   - schoonmaakmiddelen en reinigingsmiddelen voorzien van Europees Ecolabel of gelijkwaardig;
   - spieën van verschillende afmetingen;
   - persoonlijke beschermingsmiddelen voor het personeel, zoals wegwerpkleding, stofmaskers etc. Twee andere personen, niet zijnde personeel van de Opdrachtnemer, moeten ook voorzien kunnen worden van persoonlijke beschermingsmiddelen.

2. Op alle voertuigen van de Opdrachtnemer die ingezet worden bij incidentafhandelingen dient een oranje zwaailicht aanwezig te zijn dat rondom het voertuig goed zichtbaar is. Tevens dienen alle voertuigen voorzien te zijn van een trekhaak. Ter plaatse dient het gebruik van zwaailichten en andere optische signalen

conform de 'Richtlijn eerste veiligheidsmaatregelen bij incidenten' te geschieden. Tevens dienen alle voertuigen die ingezet worden te zijn voorzien van frontflitsers aan de voorzijde van het voertuig. De flitsbakken mogen alleen gebruikt worden bij het passeren van voertuigen via de vluchtstrook.

4. De Opdrachtnemer plaatst op verzoek van de calamiteitengemachtigde ter plaatse van de afhandeling een gebruiksklare mobiele lichtmast inclusief voeding.

5. Indien een botsabsorber voor de Werkzaamheden benodigd is draagt de Opdrachtnemer zorg voor het plaatsen, in stand houden en verwijderen hiervan.

C.2.7 Personeel, uitrusting, opleiding

1. De Opdrachtnemer stelt vijf categorieën medewerkers ter beschikking:
    1. Coördinator Opdrachtnemer, zoals beschreven in lid 3;
    2. Algemene ondersteuning, zoals beschreven in lid 4;
    3. Veiligheidsadviseur, zoals beschreven in lid 5;
    4. Milieudeskundige bodem en water, zoals beschreven in lid 6.
    5. Kostendeskundige raming ten behoeve van de garant- c.q. borgstelling bij een scheepsaanvaring, zoals beschreven in lid 9."

2. De Opdrachtnemer stelt het benodigde personeel ter beschikking ten behoeve van technische ondersteuning, het plaatsen van verkeersmaatregelen, schoonmaak- en herstelwerkzaamheden, bediening van het materieel en andere voorkomende Werkzaamheden.

3. De coördinator van de Opdrachtnemer is ter plaatse, of op de locatie waar hij door de Opdrachtgever is heen gestuurd, de contactpersoon van de Opdrachtnemer en is namens deze beslissingsbevoegd. De coördinator begeleidt en houdt toezicht op de Werkzaamheden, leveringen en ondersteuning van de Opdrachtnemer. De coördinator is in staat om een deskundige inschatting te maken van de risico's van de uit te voeren Werkzaamheden. De coördinator adviseert de calamiteitengemachtigde over de aanpak en stelt zich actief op tijdens de afhandeling. De coördinator moet aantoonbaar beschikken over:
    - Kennis van de CROW-richtlijnen 96a en 96b;
    - Kennis van relevante Arbo-, milieu- en veiligheidsvoorschriften;
    - Een geldig certificaat van de PBNA-opleiding 'Verkeersmaatregelen' of gelijkwaardig zoals NVVA of CROW en moet dit ter plaatse kunnen tonen;
    - Een geldig diploma Basisveiligheid VCA VOL en moet dit certificaat ter plaatse kunnen tonen.

    De coördinatoren moeten de Nederlandse taal beheersen in woord en geschrift en beschikken over goede contactuele vaardigheden.
    Bij incidenten waarbij gevaarlijke stoffen betrokken zijn, dient de coördinator Opdrachtnemer aantoonbare kennis te hebben van het beveiligen, verpakken, overladen/-pompen en afvoeren van gevaarlijke stoffen.
    De Opdrachtnemer moet altijd minimaal één coördinator beschikbaar hebben voor inzet binnen de gestelde responstijden.

4. De algemene ondersteuning betreft werknemers die zelfstandig de Werkzaamheden uitvoeren onder verantwoordelijkheid van de Opdrachtnemer. De Opdrachtnemer moet te allen tijde minimaal vier medewerkers algemene ondersteuning ter plaatse ter beschikking kunnen stellen binnen de gestelde responstijd. De werknemer algemene ondersteuning moet de Nederlandse taal spreken en in het bezit zijn van een geldig certificaat Basisveiligheid VCA of gelijkwaardig dat hij ter plaatse op verzoek moet kunnen tonen.

    Minimaal één algemene medewerker die gehouden is aan de responstijd dient

Vertrouwelijkheid: RWS INFORMATIE

over een vervoermiddel te beschikken met handgereedschap en een laadvermogen van ten minste 2.500 liter of 1.000 kg.

5. De Veiligheidsadviseur is in het bezit van een diploma Middelbare Veiligheidskunde of Hogere Veiligheidskunde of gelijkwaardig. De Veiligheidsadviseur is in het bezit van het vakbekwaamheidscertificaat Veiligheidsadviseur vervoer gevaarlijke stoffen, zoals bedoeld in de regeling Veiligheidsadviseur vervoer gevaarlijke stoffen die per 31 december 1999 van kracht is (Regeling van de Minister van Verkeer en Waterstaat van 15 januari 1999, nr. DGG/j-99000772, gepubliceerd in de Staatscourant nr. 43 1999). De Opdrachtnemer moet te allen tijde minimaal één Veiligheidsadviseur beschikbaar hebben voor inzet binnen de gestelde responstijden.

6. De milieudeskundige bodem en water moet werkzaam zijn bij een organisatie die gecertificeerd is voor de beoordelingsrichtlijnen SIKB 2000 en SIKB 6000 of gelijkwaardig en moet bevoegd zijn om de daarin vallende handelingen uit te voeren. De Opdrachtnemer moet te allen tijde minimaal één milieudeskundige beschikbaar hebben voor inzet binnen de gestelde responstijden.
   De milieudeskundige is in staat om de aard en omvang van de verontreiniging te bepalen, alsook gevraagd en ongevraagd te adviseren over de te nemen maatregelen om de verontreiniging in te perken en op te ruimen. De milieudeskundige stelt een plan van aanpak voor aan de Opdrachtgever en eventuele andere vertegenwoordigers van andere betrokken overheid(s)instanties, inclusief een tijdsplanning.
   De milieudeskundige organiseert en begeleidt het inperken en het opruimen van de milieuverontreiniging alsook het bijbehorende onderzoek conform de geldende wet- en regelgeving.

7. Personeel van de Opdrachtnemer dat de handelingen met betrekking tot gevaarlijke stoffen coördineert of uitvoert dient in het bezit te zijn van een geldig certificaat Vakbekwaamheid Gevaarlijke stoffen conform de Wet gevaarlijke stoffen en moet dat ter plaatse kunnen tonen.

8. Personeel van de Opdrachtnemer dat handelingen verricht met betrekking tot het plaatsen en coördineren van verkeersmaatregelen, dient aantoonbaar kennis te hebben van de CROW publicaties , 96a en 96b.

9. De kostendeskundige dient bij een scheepsaanvaring, op verzoek van de Opdrachtgever, een raming op te stellen ten behoeve van het vaststellen van de hoogte van de garant- c.q. borgstelling die de Opdrachtgever eist van de schadeveroorzaker c.q. van de verzekeraar van de schadeveroorzaker.

   De raming dient de globale kosten te omvatten bestaande uit:
   1. de kosten voor het veiligstellen en beschikbaarstellen van het Areaal, onderbouwd in materieel, materiaal en personeel;
   2. de kosten voor het definitief herstel, onderbouwd in materieel, materiaal en personeel;
   3. de BTW.

   De raming dient binnen twee uur na het verzoek van de Opdrachtgever digitaal te worden geleverd aan de Opdrachtgever. In die gevallen dat de ontstane schade aanleiding geeft voor het overschrijden van deze leveringstermijn, kan in overleg en overeenstemming met de Opdrachtgever een nieuwe termijn worden overeengekomen.

   De kostendeskundige dient op verzoek van de Opdrachtgever de raming toe te lichten aan de Opdrachtgever en/of aan de vertegenwoordiger van de schadeveroorzaker.

C.2.8 Milieukundige Werkzaamheden, begeleiding en transport

1. Het bodemonderzoek moet uitgevoerd worden door een organisatie die gecertificeerd is voor de beoordelingsrichtlijn SIKB 2000 (zie www.sikb.nl) of gelijkwaardig.

2. De milieukundige begeleiding en evaluatie van bodemsaneringen moeten uitgevoerd worden door een organisatie die gecertificeerd is voor de beoordelingsrichtlijn SIKB 6000 norm (zie www.sikb.nl) of gelijkwaardig.

3. Onderzoek aan bodem- en watermonsters moet uitgevoerd worden door onderzoekslaboratoria met de NEN-EN-ISO 17025 norm van de raad van accreditatie.

4. Bodemsanering moet uitgevoerd worden door een organisatie die gecertificeerd is voor de beoordelingsrichtlijn SIKB 7000 (zie www.sikb.nl) of gelijkwaardig.

5. Verontreinigde grond moet vervoerd worden naar en bewerkt worden door een organisatie die gecertificeerd is voor de beoordelingsrichtlijn SIKB 7500 (zie www.sikb.nl) of gelijkwaardig.

6. Het vervoer van afvalstoffen of gevaarlijke (afval)stoffen moet uitgevoerd worden door een bedrijf dat is vermeld op de Registratie van vervoerders, inzamelaars, handelaars en bemiddelaars van afvalstoffen (VIHB, zie www.niwo.nl) of gelijkwaardig.

C.2.9 Rapportageverplichting

Na iedere calamiteitafhandeling wordt door de Opdrachtnemer een rapportage aan de Opdrachtgever verstrekt. Deze rapportage omvat ten minste de volgende elementen:

- het zaaknummer;
- datum en tijdstip van de initiële opdracht, inclusief de naam van de calamiteitengemachtigde;
- een beschrijving van de initiële opdracht en eventuele aanvullende opdrachten;
- datum en tijdstip van het ter plaatse komen van de coördinator Opdrachtnemer of, indien geen coördinator Opdrachtnemer ter plaatse is geweest, het tijdstip waarop de Opdrachtnemer door een andere vertegenwoordiger ter plaatse kwam;
- de locatie van de calamiteit;
- een korte omschrijving van de calamiteit;
- beschrijving van beschadigde rijksobjecten, weg en wegmeubilair;
- een beschrijving van de gevolgde aanpak;
- per uitgevoerde activiteit en ingezet materieel aangeven: het tijdstip van ter plaatse komen en het tijdstip van afronding;
- datum en tijdstip waarop de laatste activiteit door de Opdrachtnemer is afgerond;
- indien van toepassing een beschrijving van de afgevoerde (afval)stoffen, materialen en andere vaste en vloeibare stoffen, de wijze waarop deze stoffen zijn getransporteerd inclusief de bestemming waar deze stoffen naar toe zijn gebracht, inclusief de benodigde afvalstroomnummers en kopieën van bewijsmateriaal (ten minste de weeg- c.q. afgiftebonnen) voor het aanleveren van de stoffen op de plaats van bestemming;
- een opgave van ingezet materieel, personeel en verwerkte materialen/hulpstoffen;
- duidelijke foto’s van de calamiteit/het incident met een minimale resolutie van 5 Megapixels, ten minste van de aangetroffen situatie, de schade aan de infrastructuur, de afgevoerde stoffen en de situatie zoals deze door de Opdrachtnemer werd achtergelaten;

Vertrouwelijkheid: RWS INFORMATIE

- indien van toepassing een beschrijving van de verwerking en de analyseresultaten van genomen grond- en watermonsters, inclusief een beoordeling van de eventueel uitgevoerde sanering/opruimwerkzaamheden;
- een fixed-price aanbieding voor het volledige (resterende) herstel van alle schade die het gevolg van de betreffende calamiteit;
- telefoonnummer van de betrokken coördinator-Opdrachtnemer of, als geen coördinator-Opdrachtnemer bij de afhandeling betrokken is geweest, van een andere contactpersoon van de Opdrachtnemer.

De rapportage dient digitaal, in Word- of Pdf-formaat, te worden geleverd. Bij de rapportage dient ook al het fotomateriaal dat de Opdrachtnemer gedurende de afhandeling heeft gemaakt te worden aangeleverd.

C.3 Voorkomende Werkzaamheden definitief herstel

C.3.1 Werkzaamheden en eisen aan geleiderail in aardebaan

1. Onder het **'**herstellen van geleiderail in aardebaan' wordt verstaan:
   Het vervangen van beschadigde geleiderailonderdelen van hetzelfde type door nieuwe, reno of herbruikbare geleiderail onderdelen. Inclusief alle benodigde leveranties en arbeid en afvoer van alle afkomende (verbindings)middelen en het uitrichten en op hoogte stellen van het vervangen gedeelte.

2. Alle te leveren c.q. te verwerken materialen dienen in de prijs per eenheid te zijn begrepen met uitzondering van de materialen zoals omschreven in lid 5 van deze paragraaf.

3. De herstelwerkzaamheden dienen te gebeuren met nieuwe, reno of herbruikbare materialen met uitzondering van bevestigingsmiddelen die te allen tijde nieuw dienen te zijn.

4. Het horizontaal en verticaal alignement van de geleiderail moet vloeiend zijn.

5. Leveranties van anti verblindingschermen, overstapconstructies, motorbeveiligingsplanken en leuningen, al dan niet geconserveerd, worden op basis van netto factuur, verhoogd met 10% Opdrachtnemersvergoeding, verrekend.

6. De technische ontwerplevensduur van nieuw geleiderailmateriaal moet ten minste 20 jaar bedragen.

7. Geleiderailconstructie met een horizontale afwijking > 250 mm van de rechtstand dient te worden hersteld.

8. De Opdrachtnemer moet er voor zorgen dat wordt voldaan aan het gestelde in het "Handboek Bermbeveiligingsvoorzieningen" en de norm NEN-ENV 1090 "Vervaardigen van staalconstructies".

9. De Opdrachtnemer dient er rekening mee te houden dat in voorkomende gevallen, waarbij een spoedschade niet direct hersteld kan worden, eerst een noodvoorziening moet worden getroffen middels het plaatsen van een tijdelijke barrier voorzien van snelkoppelingen; dit wordt bepaald door de calamiteitengemachtigde en zal direct bij melding van de spoedschade worden medegedeeld.
   De Opdrachtnemer dient er rekening mee te houden dat in voorkomende gevallen, waarbij een spoedschade niet direct hersteld kan worden, dit op dezelfde dag binnen de werkbare uren (bijlage D "Werkbare uren (WBU) en werkvensters" bij de Vraagspecificatie) moet worden hersteld. Het tijdstip van herstel wordt door calamiteitengemachtigde bepaald en zal direct bij melding van de spoedschade

worden meegedeeld.

C.3.2 Werkzaamheden en eisen aan geleiderail op kunstwerken

1. Onder het 'herstellen van geleiderail op kunstwerken' wordt verstaan: het vervangen van beschadigde geleiderail onderdelen door nieuwe geleiderail onderdelen. Inclusief alle benodigde leveranties en arbeid en afvoer van alle afkomende (verbindings)middelen.

2. Alle te leveren c.q. te verwerken materialen dienen in de eenheidsprijs te zijn begrepen met uitzondering van de materialen zoals omschreven in lid 5 van deze paragraaf.

3. Het horizontaal en verticaal alignement van de geleiderail moet vloeiend zijn.

4. Op kunstwerken dient het boren van ankergaten bij de Werkzaamheden inbegrepen te zijn.

5. Leveranties van anti verblindingschermen, overstapconstructies en leuningen, al dan niet geconserveerd, worden op basis van netto factuur, verhoogd met 10% Opdrachtnemersvergoeding, verrekend.

6. De Opdrachtnemer moet er voor zorgen dat wordt voldaan aan het gestelde in het "Handboek Bermbeveiligingsvoorzieningen" en de norm NEN-ENV 1090 "Vervaardigen van staalconstructies".

7. De technische ontwerplevensduur van nieuw geleiderailmateriaal moet ten minste 20 jaar bedragen.

C.3.3 Werkzaamheden en eisen aan uitrichten en op hoogte stellen van geleiderail

1. Onder het 'uitrichten en op hoogte stellen' van geleiderail wordt verstaan: Het op een correcte hoogte en in juiste rechtstand brengen van alle voorkomende enkele en/ of dubbele geleiderail, met uitzondering van geleiderail op kunstwerken, zoals beschreven in "Handboek Bermbeveiligingsvoorzieningen 2000, uitgave CROW september 2000".

2. Geleiderailconstructie met een horizontale afwijking > 250 mm van de rechtstand dient te worden hersteld.

3. Bij het uitrichten en op hoogte stellen behoort eveneens het leveren en aanbrengen van anti-verzakkingsplaten.

C.3.4 Werkzaamheden en eisen aan het herstellen van asfalt- en voegconstructieschade

1. Onder het 'herstellen van asfaltschade' wordt verstaan: het vervangen van beschadigde (delen van) asfaltdeklagen door een nieuw aan te brengen deklaag, inclusief alle benodigde leveranties, arbeid, stort- en/of verwerkingskosten.

2. Het herstellen van asfaltschade betreft alle voorkomende schades in de deklagen. Aanwezig in het werkgebied is o.a. Asfaltbeton AC-surf, Zeer Open Asfalt Beton (ZOAB), Steen Mastiek Asfalt (SMA) en combinatiedeklagen.

3. De asfaltsamenstelling dient functioneel en kwalitatief en qua samenstelling en eigenschappen minimaal gelijkwaardig te zijn aan de verwijderde asfaltdeklagen.

4. Tot het herstellen van de asfaltschade behoort ook het aanbrengen en herstellen

Vertrouwelijkheid: RWS INFORMATIE

van markeringen, het vervangen van detectielussen en detectoren en andere in de verharding aanwezige onderdelen.

5. Bij het verwijderen en vervangen van de asfaltconstructie op kunstwerken dient de Opdrachtnemer er rekening mee te houden dat de belasting per m2 van de nieuwe constructie nooit meer bedraagt dan de belasting per m2 van de oude constructie. De Opdrachtnemer moet zodanige maatregelen treffen dat er geen water op het kunstwerk blijft staan. De afvoer van het water mag geen uitspoeling tot gevolg hebben.

6. Voor zover niet aanwezig moet de Opdrachtnemer ter plaatse van de voegconstructies tussen de schampkanten en de aan te brengen asfaltconstructie een waterdichte constructie aanbrengen (maximaal 2,0% holle ruimte). In geval van een open deklaag mag deze waterdichte constructie niet hoger zijn dan de onderzijde van de open deklaag.

7 Bij reparatie van een voegconstructie moet de nieuwe voegconstructie gelijksoortig zijn. Materiaalverlies en/of tekenen van onthechting mogen niet voorkomen. De bovenzijde van de nieuwe asfaltdeklaag moet over ten minste 1,0 m breedte op gelijke hoogte c.q. in profiel aansluiten aan de bovenzijde van de voegconstructie. De maximaal toegestane afwijking hierbij bedraagt 5 mm.

8. De langsnaden in de bovenlaag asfalt moeten strak en in een rechte lijn worden uitgevoerd en mogen niet minder dan 0,05 m en niet meer dan 0,20 m naast een as- of deelstreep zijn gelegen.
   Het is toegestaan een langsnaad aan te brengen in een gedeelte ter breedte van 1,0 m in de as van de rijstrook; deze langsnaad moet strak en in rechte lijn worden uitgevoerd. In dat geval moet de betreffende rijstrook, voordat deze voor het openbaar verkeer wordt opengesteld, over de totale breedte zijn vervangen.

9. De opeenvolgende lagen asfalt zodanig aanbrengen dat de langsnaden of dwarsnaden ten minste 0,15 m uit elkaar liggen, indien mogelijk trapsgewijs.
   In de onderlagen of tussenlagen van een rechterrijstrook (gezien in de rijrichting), met uitzondering van een gedeelte ter breedte van 1,0 m in de as daarvan, mogen in het asfalt geen langsnaden voorkomen.

C.3.5 Werkzaamheden en eisen aan het herstellen van krasschades

1. Onder het 'herstellen van krasschade' wordt verstaan:
   het herstellen van, door mechanisch geweld aangebrachte, langs- en dwarsgroeven in de asfaltdeklagen inclusief alle benodigde leveranties en arbeid.

2. Indien de krasschade kan worden hersteld met een reparatiemiddel dient de Opdrachtnemer de geschiktheid vóór toepassing aan te tonen. Hierbij dient aangetoond te worden dat het reparatiemiddel:
   - gedurende de gehele (resterende) technische levensduur van de deklaag waarin of waarop zij worden toegepast ten minste even stroef is als die deklaag;
   - geen geleidend effect heeft op het verkeer dat conflicteert met de beoogde wegindeling etc. (conform componentspecificatie bovenbouw, SOA 2014, paragraaf 8.3.5).

C.3.6 Werkzaamheden en eisen aan het verrichten van eenvoudige betonreparaties

1. Onder het 'verrichten van eenvoudige betonreparaties' wordt verstaan:
   het herstellen van schades op en aan kunstwerken van beton waarbij de wapening niet is beschadigd, inclusief alle benodigde leveranties, materieel en arbeid.

2. De schade dient hersteld te worden met een hiertoe bestemde krimparme reparatiemortel.

3. Het gebruik van epoxymortels is niet toegestaan.

4. Het hulpmaterieel moet voldoen aan de wettelijke veiligheidsvoorschriften. Indien de Opdrachtnemer voor het toepassen van hulpmaterieel gebruik wenst te maken van het terrein van overige beheerders, dient hij hiervoor toestemming te vragen bij de desbetreffende beheerder.

5. Voor het steigermaterieel dient te worden gerekend met een doorrijhoogte van ten minste 4 m en geleiderail met leuningconstructie (900 mm ten opzichte van het inspectiepad).

C.3.7 Werkzaamheden en eisen aan het uitwisselen van RIMOB's

1. Onder het 'uitwisselen van een RIMOB' wordt verstaan:
het binnen 24 uur vervangen van een (deels) beschadigde rimpelbuis obstakelbeveiliger door een onbeschadigd exemplaar, inclusief alle benodigde leveranties en arbeid.

2. Het uitwisselen van RIMOB's is exclusief betonfundering.

3. De te plaatsen RIMOB's mogen slechts samengesteld worden uit nieuwe of renomaterialen.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage D Werkbare Uren (WBU)

De tabel met WBU voor vaarwegen:

vaarweg	*openstelling*	*WBU*
HTA (Hoofdtransportas)	7 x 24 uur	Geen
HVW (Hoofdvaarweg)	7 X 24 uur	Geen
HVW (Geen 24-uurs bediening of beperkte bediening)	Werkdagen 5 x 24 uur Weekend 2 x (06:00 - 22:00)	Geen Vr – Za 24:00 - 06:00 Za – Zo 22:00 - 06:00 Zo – Ma 22:00 - 06:00
OVW (overige vaarwegen)	7 X 24 uur	Geen
OVW (Geen 24 uurs bediening of beperkte bediening)	Werkdagen 06:00 - 07:00 en 09:00 - 16:00 en 19:00 - 20:00 Weekend 00:00 – 24:00	Werkdagen 20:00 - 06:00 Kortdurende hinder < 2 uur in de ochtend- & avondspertijd

De Opdrachtgever kan de tabel jaarlijks aanpassen. Daarnaast kan het contract aanvullende en/of andere eisen stellen t.a.v. werkbare uren.
In toevoeging op de informatie in de tabel met WBU mogen op de volgende dagen en tijdstippen geen werkzaamheden uitgevoerd worden:

- Nieuwjaarsdag
- Vanaf Toede Vrijdag t/m Tweede Pasen
- 27 april Koningsdag
- 4 mei vanaf 14.00 uur tot 6 mei 10.00 uur;
- Woensdag voorafgaand aan het Hemelvaartsweekend t/m zondag;
- Vrijdag voorafgaand aan het Pinksterweekend t/m Tweede Pinksterdag
- 24 t/m 26 december

Bijlage E Slot’s

De door de Opdrachtgever bepaalde Slot’s voor rijksvaarwegen.

Rijksvaarweg	Locatie	Dag	Tijdstip: van …	…tot
<vul voorgeschreven Slot in>				

Niet van toepassing

Vertrouwelijkheid: RWS INFORMATIE

Bijlage F Aanvragen verkeersmaatregelen

Conform Protocol Vaarwegen herziene versie 2018

Bijlage G Overzicht ten behoeve van Activiteiten

Voorgeschreven Activiteiten

Nummer	Omschrijving
G-0.1	Bathse Spuisluis - conservering damwand boven de waterlijn - vervanging no-break systeem - werkzaamheden aan centrale bedieningsgebouw
G-0.2	Gemaal Kreekrak - vervangen van brand- & ontruimingsinstallatie, vluchtweginstallatie, debietmeetinstallatie, elektrotechnische installatie, bedienings- en besturingsinstallatie, laagspanningsinstallatie, objectverlichting - tegelwerk gebouw - diverse conserveringswerkzaamheden: krooshoek, damwand, leuningen, schuiven & schuifconstructies - bodembescherming - dilatatievoegen deksloof - hefinrichting, terugslapklep, elektromotor en vijzel persschuiven 2 t/m 5
G-0.3	Grevelingensluis - werkzaamheden aan gebouw
G-0.5	Kanaal door Zuid-Beveland - vervangen aanstraalverlichting
G-0.6	Post- en Vlakebrug - werkzaamheden aan tandheugels, schotelveren, remvijzels, hoofddraaipunten, schamelstel en noodstroomaggregaat
G-0.7	Kreekraksluizen Civiel - werkzaamheden bedieningsgebouw en inlaatgebouw - werkzaamheden aan toegang tot bepaalde voorzieningen - vervangen bebording en drijfmiddelen - bodembescherming - vervangen damwand - diverse conserveringswerkzaamheden: leuningwerk, bolders/haalkommen, bedrijfschuiven en noodsschuiven, hoofddraagconstructie, onderhoudsschuiven - vervangen dilatatievoegvullingen - werkzaamheden heftorens - werkzaamheden aan wegdek bruggen - vervangen bestaande verharding diverse wegen
G-0.8	Kreekraksluizen EIA - vervangen hefmotor, elektromotoren - vervangen binnenverlichting, verlichting & noodverlichting op complex - diverse duurzaamheidsmaatregelen - laagspanningsverdeler inlaatwerk en uitlaatwerk - sleutelbeheer - masten vervangen + bliksembeveiligingsinstallatie

Vertrouwelijkheid: RWS INFORMATIE

	- vervangen laagspanningkasten - vervangen laagspanning bedieningsgebouw
G-0.9	Kreekraksluizen WTB - werkzaamheden aan: remvijzels, taats- en droogzetkuip, schuif-aandrijvingen en- en uitlaatwerk en hoofddraagconstructie

Optionele Activiteiten

Nummer	Omschrijving
G-0.3	Grevelingensluis - conservering afsluitboomkasten
G-0.4	Noordwestelijke Delta: dammen, dijken, oevers Diverse werkzaamheden waaronder: - Verwijderen opschot, houtachtige vegetatie, onkruid en invasieve exoten - bestrijden graverij - aanbrengen inwasmateriaal
G-0.7	Kreekrak Civiel: - conservering deuren, bedrijfschuiven, noodschuiven en onder-houdsschuiven
G-0.8	Kreekrak EIA - werkzaamheden bedieningsgebouw: luchtbehandelingsinstallatie, laagspanningsinstallatie, noodverlichting - vervangen radarinstallatie
G-0.9	Kreekrak WTB - vervangen haalkabels, omloopkabels en buffers
G-0.10	Levering bedienplekken

G.1 Raamactiviteiten

Het overzicht van de Raamactiviteiten is opgenomen in een afzonderlijk format "Overzicht Raamactiviteiten"

Vertrouwelijkheid: RWS INFORMATIE

Bijlage H Projectrisicolijst

Niet van toepassing i.v.m. Best Value

Bijlage I Reinigen van zeer open asfaltbeton

I.1 Begripsbepaling

Het reinigen van ZOAB bestaat uit het doorspuiten van de ZOAB met water onder hoge druk waarbij het uit de ZOAB tredende vuilwatermengsel direct wordt opgezogen en opgevangen. Na bezinking worden water en bezinksel onderzocht op samenstelling en verontreiniging voor verdere verwerking.

I.2 Materieel

Het in te zetten reinigingsvoertuig moet zijn voorzien van een reinigingsbalk met een minimale lengte van 2,40 m. Het reinigingsmechaniek heeft zowel sproeimogelijkheden (sproeikoppen) als zuigmogelijkheden en is zodanig aangebracht, dat het wegoppervlak over de gehele lengte van het reinigingsmechaniek kan worden gereinigd. De waterdruk bedraagt minimaal 7 MPa en maximaal 13 MPa en is vanaf het voertuig in te stellen en af te lezen.

Het te gebruiken sproeiwater moet vrij zijn van oliën, vetten en vaste, zwevende of drijvende bestanddelen.

I.3 Uitvoering

Het reinigen gebeurt met een werkdruk van 10 MPa. Daarbij rijdt het voertuig met een snelheid van maximaal 2 km/u.

Het uittredende vuilwatermengsel moet in een tank worden opgevangen. Na bezinking van het vuil moeten het water en bezinksel elk afzonderlijk worden onderzocht op samenstelling en verontreiniging. Voor het bezinksel gebeurt dat per afgifte van 10 m^3. Daarna moeten water en bezinksel worden afgevoerd naar de desbetreffende verwerkingslocatie.

Bij temperaturen van 5ºC of lager of bij kans op nachtvorst mag niet worden gereinigd.

I.3.1 Uitvoeringsplan

Voorafgaand aan het reinigen van ZOAB moet een uitvoeringsplan worden opgesteld waarin ten minste de keuzen worden vastgelegd voor:

- maximale waterdruk en debiet van de sproei-installatie alsmede de zuigcapaciteit van de zuigpomp van het te gebruiken voertuig;
- de herkomst van het te gebruiken water ten behoeve van de reiniging;
- de locatie waar het vervuild water wordt verwerkt;
- de locatie waar het bezinksel wordt verwerkt;
- de reinigingstijdstippen.

Het uitvoeringsplan dient ter Acceptatie te worden aangeboden.

I.3.2 Verantwoordingsrapportage

Jaarlijks overlegt de Opdrachtnemer een rapportage van de reinigingswerkzaamheden in het afgelopen jaar. Deze rapportage moet ten minste omvatten:

- een overzicht in Excel van de wegvakken gerangschikt naar wegnummer, rijrichting, kilometrering en gereinigde strook met daarin aangegeven de tijdstippen van reinigen;
- een door derden verzorgde rittenadministratie van de ingezette reinigingsvoertuigen gebaseerd op gps-tripmaster gegevens;
- keuringsrapportages van het opgezogen water en bezinksel;
- afleverbewijzen van het vervuilde water en bezinksel bij de verwerkingslocaties.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage J Beoordelingsmethodiek schade bovenbouw en onderbouw

Ernst van de schade

De ernst van schade aan bovenbouw en onderbouw wordt ingedeeld in vier klassen (zie onderstaande tabellen 1 t/m 3).

Tabel 1

Schadevorm	Ernstklasse			
	I	**II**	**III**	**IV Spoedeisende schade**
Dwarsscheuren[1] wijdte en/of hoogteverschil	 < 3 mm < 2 mm	 3 t/m 20 mm 2 t/m 10 mm	 21 t/m 30 mm 11 t/m 15 mm	 > 30 mm > 15 mm
Langsscheuren[1] Wijdte en/of hoogteverschil	 < 3 mm < 2 mm	 3 t/m 20 mm 2 t/m 10 mm	 21 t/m 30 mm 11 t/m 15 mm	 > 30 mm > 15 mm
Craquelé	scheuren niet verbonden	scheuren verbonden, geen losse elementen	scheuren verbonden met losse elementen	zie klasse III

[1] per individuele scheur

Tabel 2

Schadevorm	Ernstklasse			
	I	**II**	**III**	**IV Spoedeisende schade**
Rafeling Op Open Deklaag	6 t/m 10% van eerste steenlaag weg[1]	11 t/m 20% van eerste steenlaag weg[1]	> 20% van eerste steenlaag weg[1]	Gat conform definitie "Richtlijnen handelwijze bij noodschade"[4]
Rafeling Op Dichte Deklaag	Hier en daar mortel uit oppervlak en/of af en toe steentje weg	Meerdere steentjes weg en/of eerste steenlaag weg over beperkte schadeplek[2]	Eerste steenlaag weg over grotere schadeplek[3] en/of tweede steenlaag weg	Gat conform definitie "Richtlijnen handelwijze bij noodschade"[4]
Stroefheid Actuele stroefheidscore AS	> 0,07	0,07 t/m 0,00	-0,01 t/m - 0,06	< - 0,06
Rijspoordiepte[5]	< 10 mm gemiddeld over 100 m	10 t/m 17 mm gemiddeld over 100 m	18 t/m 22 mm gemiddeld over 100m of > 22mm gemid-	> 22mm

Tabel 2

Schadevorm	Ernstklasse			
	I	**II**	**III**	**IV Spoedeisende schade**
			deld over ≥ 50m	
Ribbelvorming[6]	< 4 mm	4 t/m 5 mm	> 5 mm	n.v.t.
Blaasvorming[7]	geen blaasvor-ming	geen blaasvor-ming	alle blaasvorming	n.v.t.

[1] voor elk aanwijsbaar oppervlak van 100 x 100 cm
[2] kleiner dan 20 x 20 cm
[3] 20 x 20 cm of groter
[4] afmetingen 20 x 20 x 5 cm of groter
[5] de rijspoordiepte is de "rut depth R" volgens NEN-EN 13036-8:2008 §6.4, bepaald met een rei met lengte 2000 mm
[6] in opstelstroken
[7] op kunstwerken

Tabel 3

Schadevorm	Ernstklasse			
	I	**II**	**III**	**IV Spoedeisende schade**
Langsonvlakheid[1] **IRI**	< 2,6	2,6 t/m 3,4	3,5 t/m 4,0	> 4,0
Hoogteverschil langsrichting[2] **□h**	< 50 mm over 25 m	50 mm over 25 m t/m 79 mm over 25 m	80 mm over 25 m t/m 149 mm over 25 m	>149 mm over 25 m
Helling dwarsrich-ting[3]	> NOA - 0,5%	NOA – 0,5% t/m NOA - 1,4%	NOA – 1,5% t/m NOA – 1,6%	< NOA – 1,6%
Hellingsverschil dwarsrichting[4]	> -0,5% en < 0,5%	-0,5% t/m -0,9% of 0,5% t/m 0,9%	-1,0% t/m -1,4% of 1,0% t/m 1,4%	< -1,4% of > 1,4%
Hellingsverschil langsrichting[5] bij overgang op kunstwerk	≥ -1:v en ≤ 1:v	<-1:v en ≥ -1:(¾v) of > 1:v en ≤ 1:(¾v)	<-1:(¾v) en ≥-1:(½v) of > 1:(¾v) en ≤ 1:(½v)	< -1:(½v) of > 1:(½v)

[1] gemiddelde waarde over 100 meter
[2] hoogteverschil over twee willekeurige punten in langsrichting ten opzichte van de situatie bij oplevering
[3] NOA staat voor de vereiste dwarshelling volgens de NOA
[4] aangegeven dwarshellingsverschillen zijn procentpunten
[5] v staat voor de ontwerpsnelheid in km/u

Omvang van de schade

Vertrouwelijkheid: RWS INFORMATIE

Omvangcategorieën
De omvang van schade wordt ingedeeld in drie categorieën (zie onderstaande tabel 4).
Deze indeling wordt gedaan per ernstklasse en per 100 meter rijstrooklengte. Hierbij worden alle schadeplekken in dezelfde ernstklasse gesommeerd.

Vervolgens wordt de gesommeerde omvang aan de hand van de navolgende tabel ingedeeld in één van de omvangcategorieën.

Tabel 4

Schade	**Omvangcategorieën**		
	X	**Y**	**Z**
Rafeling (% lengte van 100 m-vak)	< 15%	15 t/m 25%	> 25%
Dwarsscheuren (aantal binnen 100 m-vak)	< 3	3 t/m 7	> 7
Langsscheuren en/of craquelé (% lengte van 100 m-vak)	< 10%	10 t/m 30%	> 30%
Samengestelde schade[1] (% lengte van 100 m-vak)	< 15%	15 t/m 30%	> 30%

[1] combinatie van rafeling in ernstklasse II, langsscheuren in ernstklasse I en craquelé in ernstklasse I op dichte deklagen

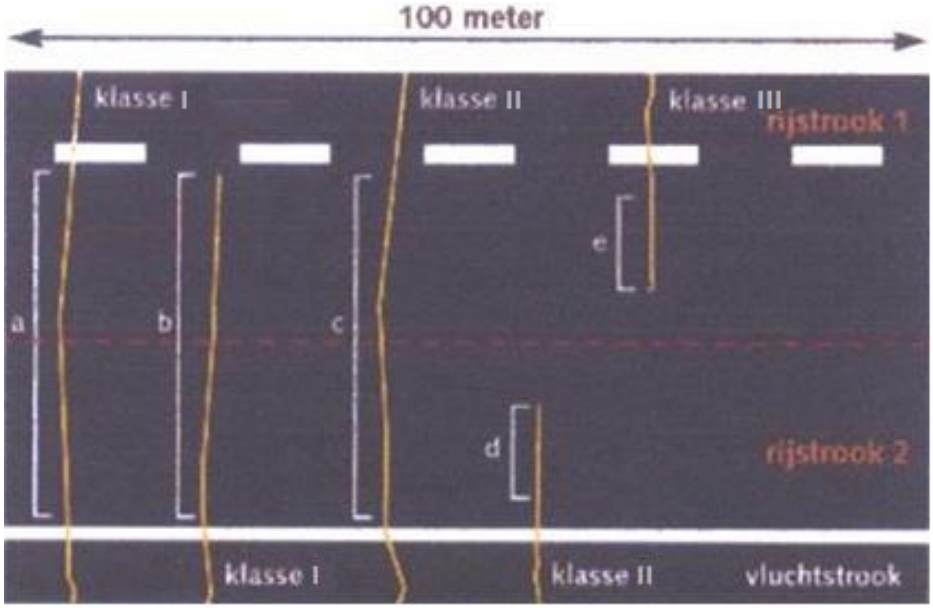
Bepaling omvang
De wijze waarop de omvang wordt bepaald is gevisualiseerd in de figuren 1 t/m 4.

- Figuur 1 laat zien hoe de omvang van dwarsscheuren wordt berekend. De scheurlengte per ernstklasse wordt opgeteld en de som wordt vervolgens gedeeld door de rijstrookbreedte.
- Bij rafeling wordt voor elke ernstklasse per rijstrookhelft het aantal strekkende meters in het rijspoor bepaald, vervolgens opgeteld en door twee gedeeld (figuur 2).
- Voor langsscheuren en/of craquelé geldt een soortgelijke aanpak. De omvang van de schade wordt per rijstrookhelft bepaald en vervolgens opgeteld, waarna de som door twee wordt gedeeld. Eerst wordt de omvang in ernstklasse III bepaald, vervolgens de omvang in ernstklasse II en tenslotte de omvang in ernstklasse I. 'Overlappende schade' in een lagere ernstklasse binnen dezelfde rijstrookhelft wordt niet meegerekend (figuur 3).
- Ook bij de combinatie van de schades rafeling, langsscheuren en craquelé wordt op deze wijze te werk gegaan. Schades in de ernstklasse II worden per rijstrookhelft getotaliseerd, vervolgens worden de totalen van beide rijstrookhelften bij elkaar opgeteld en door twee gedeeld (figuur 4).

Bij rafeling, langsscheuren en craquelé en bij de combinatie van deze schades kan de omvang van de drie ernstklassen samen maximaal 100% zijn.

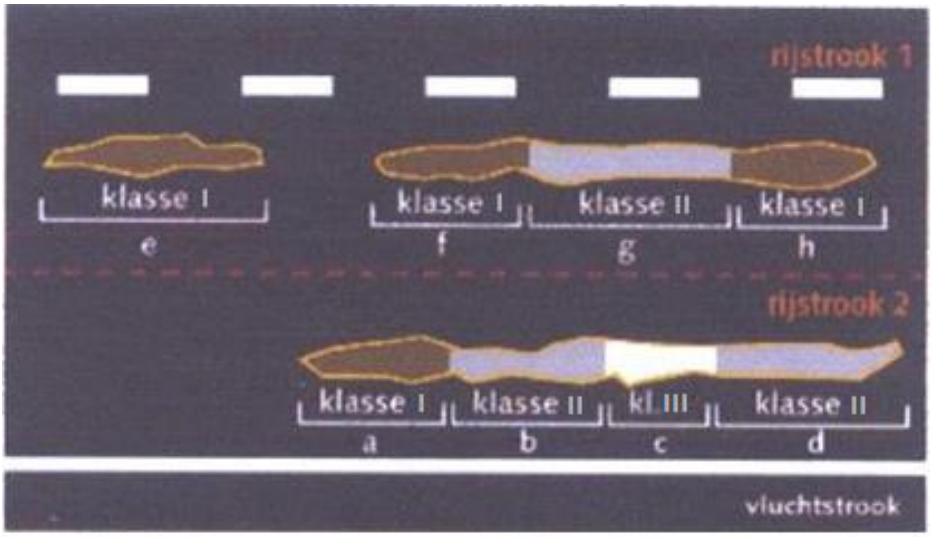
Voor de schades dwars- en langsonvlakheid, stroefheid en dwarshelling wordt geen omvang per 100 meter bepaald. Voor deze schades zijn meetwaarden beschikbaar (ARAN). Dit zijn de gemiddelde waarden per 100 meter.

Figuur 1:
Bepaling van de omvang van dwarsscheuren



Omvang ernstklasse I = (a+b) gedeeld door de breedte van strook 2
Omvang ernstklasse II = (c+d) gedeeld door de breedte van strook 2
Omvang ernstklasse III = e gedeeld door de breedte van strook 2

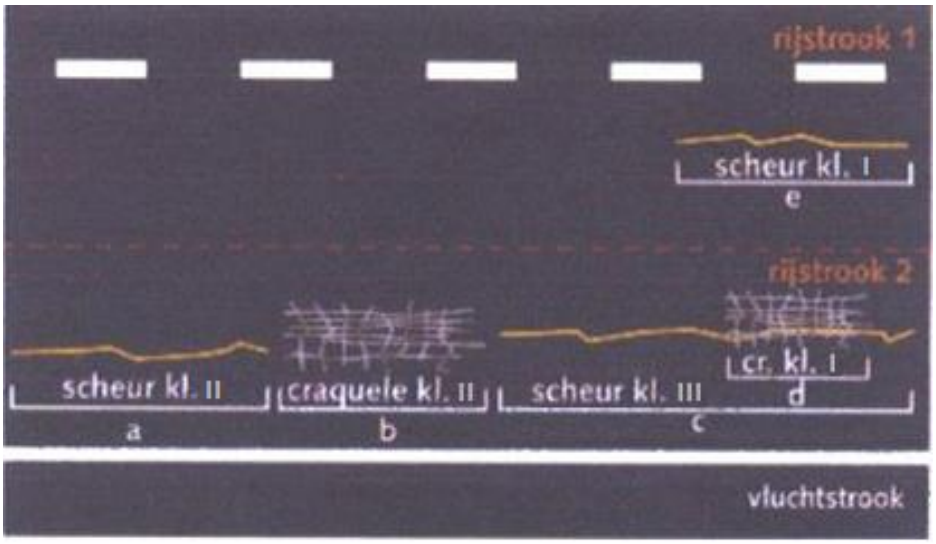
Figuur 2:
Bepaling van de omvang van Rafeling



Omvang ernstklasse I = ((a+e+f+h)/2) gedeeld door de lengte van het beschouwde rijstrooksegment
Omvang ernstklasse II = ((b+d+g)/2) gedeeld door de lengte van het beschouwde rijstrooksegment
Omvang ernstklasse III = (c/2) gedeeld door de lengte van het beschouwde rijstrooksegment

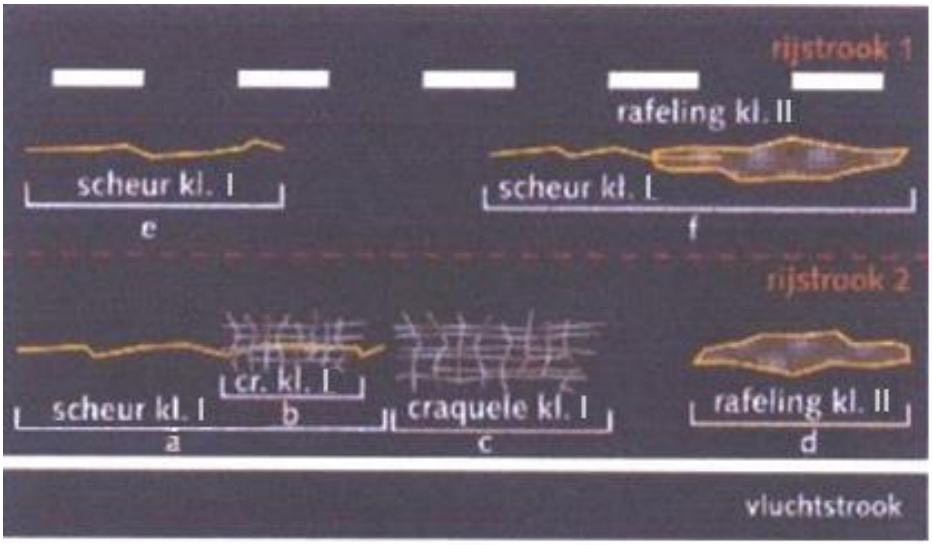
Vertrouwelijkheid: RWS INFORMATIE

Figuur 3:
Bepaling van de omvang van scheurvorming (langsscheuren en/of craquelé)



Omvang ernstklasse I = (e/2) gedeeld door de lengte van het beschouwde rijstrooksegment
Omvang ernstklasse II = ((a+b)/2) gedeeld door de lengte van het beschouwde rijstrooksegment
Omvang ernstklasse III = (c/2) gedeeld door de lengte van het beschouwde rijstrooksegment

Figuur 4:
Bepaling van de samengestelde omvang van rafeling in ernstklasse II, langsscheuren in ernstklasse I en craquelé in ernstklasse I op dichte deklagen



Omvang samengestelde schade = ((a+c+d+e+f)/2) gedeeld door de lengte van het beschouwde rijstrooksegment

Bijlage K Integraal Veiligheidsplan

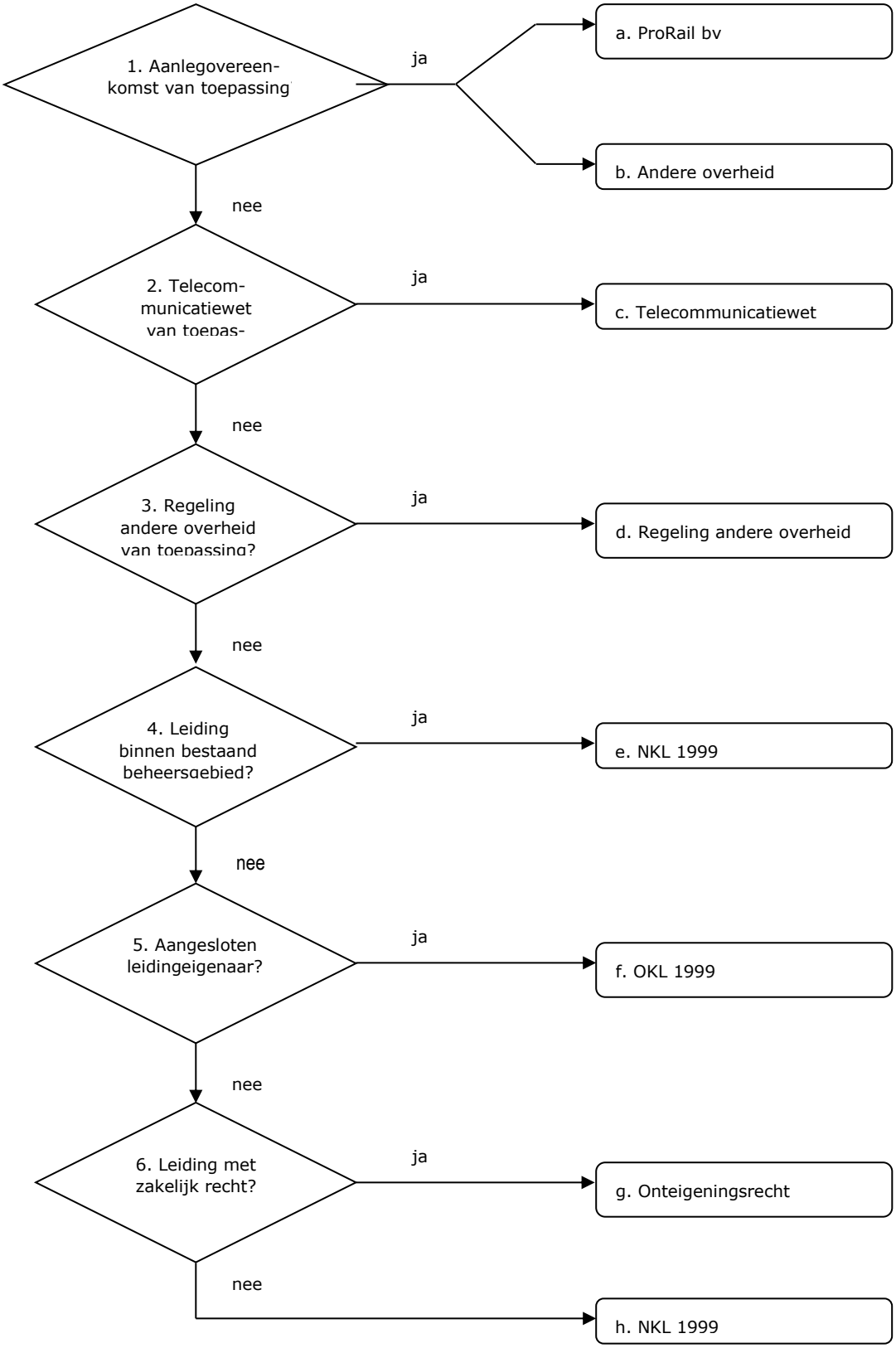
Zie separate documenten.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage L Definities integrale veiligheid

Vervallen.

Bijlage M Regelingenschema Kabels en Leidingen Derden



TOELICHTING REGELINGENSCHEMA

ad a
- ProRail bv = een overeenkomst conform het Samenwerkingsprotocol ProRail – Rijkswaterstaat d.d. 15 december 2011, op grond waarvan de Opdrachtgever alle kosten draagt van het aanpassen van de kabels en leidingen in beheer bij ProRail bv.

ad b
- Andere overheid = een overeenkomst met een andere bij de Werkzaamheden betrokken overheid, op grond waarvan de Opdrachtgever alle kosten draagt van het aanpassen van de kabels en leidingen in beheer bij die overheid.

ad c
- Telecommunicatiewet = de Telecommunicatiewet met bijbehorende Uitvoeringsprotocol Telecom d.d. 13 november 2012, inclusief de bijlagen waaronder de model-Projectovereenstemmingen (nacalculatie, vaste prijs, vereenvoudigd en geschillen) met bijlagen.
- Opmerking: KPN bv verwijdert op eigen kosten de verlaten kabels van het Wegen Telecommunicatie Netwerk, voor zover gelegen buiten het grondgebied van Rijkswaterstaat, conform het Transitieplan WTN d.d. 5 februari 2007 en de Overeenkomst voor onbepaalde tijd inzake beschikking en beheer ten aanzien van de functieloze WTN kabels d.d. 22 december 2011.

ad d
- Regeling andere overheid = een vergoedingsregeling van een andere overheid, welke wordt toegepast op een wijziging van aansluitende, kruisende of naastliggende infrastructuur van die overheid.
- Die overheid kan ook ProRail bv zijn (handelt namens de Minister van Infrastructuur en Waterstaat).
- Uitzondering: bij een ligging zonder toestemming van die overheid, dan wel in strijd met de voorschriften van de toestemming, kan het zijn dat er geen recht op vergoeding bestaat.

ad e
- NKL 1999 = de Nadeelcompensatieregeling verleggen kabels en leidingen in en buiten rijkswaterstaatswerken en spoorwegwerken 1999 (Staatscourant 1999, nr. 97) met het bijbehorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Het gaat hier om Afdeling 1.2. Recht op vergoeding voor het verleggen van kruisende en/of langsleidingen en de omvang daarvan.
- Uitzondering: bij een ligging zonder vergunning van de Opdrachtgever, dan wel in strijd met de voorschriften van de vergunning, kan het zijn dat er geen recht op vergoeding bestaat.
- Opmerking: de Defensie Pijpleiding Organisatie gaat op eigen kosten over tot het verwijderen van loze leidingen.

ad f
- OKL 1999 = overeenkomst inzake verleggingen van kabels en leidingen buiten beheersgebied tussen de Minister van Verkeer en Waterstaat (thans Infrastructuur en Waterstaat) en EnergieNed, VELIN en VEWIN (Staatscourant 1999, nr. 97) met het bijbehorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Opmerking: de Defensie Pijpleidingen Organisatie gaat op eigen kosten over tot het verwijderen van loze leidingen.

ad g

- Onteigeningsrecht = de Onteigeningswet met de bijbehorende jurisprudentie.
- Afgesproken kan worden de OKL 1999 te volgen, tenzij de kabel- of leidingbeheerder hiervoor alleen kiest in gevallen dat dit voor hem gunstig uitpakt.

ad h

- NKL 1999 = de Nadeelcompensatieregeling verleggen kabels en leidingen in en buiten rijkswaterstaatswerken en spoorwegwerken 1999 (Staatscourant 1999, nr. 97) met het bijbehorende Uitvoeringsprotocol schadevergoeding kabels en leidingen (SKL 01-26, 14 september 2001), inclusief de model-Projectovereenstemmingen (vaste prijs en nacalculatie) met bijlagen.
- Het gaat hier om Afdeling 1.3. Recht op vergoeding voor het verleggen van buitenleidingen en de omvang daarvan.
- Eigenlijk geldt deze afdeling alleen voor een kabel of leiding die valt onder één van de categorieën openbare werken als bedoeld in de Belemmeringenwet Privaatrecht. Dit zou betekenen dat op de overige kabels en leidingen niet de NKL 1999 maar de Regeling nadeelcompensatie Verkeer en Waterstaat 1999 (Staatscourant 1999, nr. 172) zou moeten worden toegepast. Omdat die regeling echter slechts algemene normen kent, zou naar alle waarschijnlijkheid toch de NKL 1999 inhoudelijk worden gevolgd.
- Er kan een lastige situatie ontstaan als de kabel- of leidingbeheerder weigert aan het Verzoek tot Aanpassing te voldoen en hiertoe ook niet door een derde partij (vaak een andere overheid) kan worden gedwongen. Alsdan zal toch in minnelijk overleg tot een vergelijk moeten worden gekomen. Daarbij kan in het uiterste geval een volledige schadeloosstelling (onteigeningsrecht) worden geboden. De kabel- of leidingbeheerder is immers niet verplicht een beroep op de NKL 1999 te doen. Wil deze een nog verdergaande vergoeding van alle huidige en toekomstige kosten, dan lijkt er toch sprake van misbruik van recht (artikel 3:13 BW) c.q. een gedraging in strijd met de zorgvuldigheid die men in het maatschappelijk verkeer tegenover elkaar heeft te betrachten (artikel 6:162 BW). In dat geval dient een kort geding te worden overwogen.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage N Richtlijn Samenwerking Rijkswaterstaat - Markt op Integrale Projecten

Vervallen.

Bijlage O Rijkswaterstaat Brede Afspraak Archeologie

Vertrouwelijkheid: RWS INFORMATIE

Bijlage P Programma van Eisen voor uitvoerend archeologisch onderzoek

Bijlage Q Rijkswaterstaat Brede Afspraak Duurzaam Inkopen

Vertrouwelijkheid: RWS INFORMATIE

Bijlage R Staat van prijzen per eenheid calamiteiten en incidenten

1. Onderstaande prijzen per eenheid zijn uitsluitend bedoeld voor calamiteiten en incidenten in het Areaal conform § 5.4.7 van de Vraagspecificatie Proces.
2. In de prijzen per eenheid zijn begrepen alle directe en indirecte kosten waaronder algemene kosten, winst en risico (akwr).
3. De prijzen per eenheid zijn vast gedurende de looptijd van de Overeenkomst.

A Verkeersmaatregel				
Volg Nr.	**Ter beschikking stellen beveiligings- en incidentmaatregelen volgens de richtlijn aanvullende incidentmaatregelen bij langer durende verkeersincidenten**	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
1	Een incidentbeveiliging bestaande uit een verzwaarde actiewagen met automatische andreasstriplegger, inclusief andreasstrips en 10 verkeerskegels op een rijbaan met rijstrooksignalering op een A-weg	30	Keer	€ 800
2	Een incidentbeveiliging bestaande uit een verzwaarde actiewagen met automatische andreasstriplegger, inclusief andreasstrips en 10 verkeerskegels met 3 voorwaarschuwingswagens op een rijbaan zonder rijstrooksignalering tijdens daglicht op een A-weg	30	Keer	€ 1.050
3	Een incidentbeveiliging bestaande uit een verzwaarde actiewagen met automatische andreasstriplegger, inclusief andreasstrips en 10 verkeerskegels met 3 voorwaarschuwingswagens (VMS) op een rijbaan zonder rijstrooksignalering na zonsondergang op een A-weg	30	Keer	€ 2.143
4	Een incidentbeveiliging bestaande uit een verzwaarde actiewagen met automatische andreasstriplegger, inclusief andreasstrips en 10 verkeerskegels op een N-weg	30	Keer	€ 800
5	Het afsluiten van een rijstrook of in-/uitvoegstrook op een N-weg	120	Keer	€ 840
6	Incidentmaatregel voor Werkzaamheden in de berm binnen de obstakelvrije zone tot 3,5 meter van de kantstreep	120	Keer	€135
7	Incidentmaatregel voor Werkzaamheden waarbij de vluchtstrook, en eventueel de uitvoegstrook, moet worden afgezet met rijstrooksignalering boven de rijbaan	120	Keer	€ 755
8	Incidentmaatregel voor Werkzaamheden waarbij de vluchtstrook, en eventueel de uitvoegstrook, moet worden afgezet zonder rijstrooksignalering boven de rijbaan	120	Keer	€ 740

A Verkeersmaatregel				
Volg Nr.	**Ter beschikking stellen beveiligings- en incidentmaatregelen volgens de richtlijn aanvullende incidentmaatregelen bij langer durende verkeersincidenten**	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
9	Incidentmaatregel voor Werkzaamheden waarbij 1 rijstrook moet worden afgezet met rijstrooksignalering boven de rijbaan	120	Keer	€ 740
10	Incidentmaatregel voor Werkzaamheden waarbij 1 rijstrook moet worden afgezet met inzet van 2 TRS-sen	120	Keer	€ 2.400
11	Incidentmaatregel voor Werkzaamheden waarbij 2 rijstroken moeten worden afgezet met inzet van 3 TRS-sen	120	Keer	€ 3.300

Opmerking: Bij calamiteiten/incidenten waar 2 of meer rijstroken dienen te worden afgezet, de posten 1 en 9 vermenigvuldigen met het aantal af te zetten rijstroken.

B Vaarwegverkeersmaatregel				
Volg Nr.	**Ter beschikking stellen Vaarwegincidentmaatregelen**	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
1			Keer	€
2			Keer	€

C Ondersteunende veiligheidsmaatregelen / verkeersmaatregelen / personeel				
	Overige / personeel inclusief kosten van transport, gereedschappen en klein materiaal	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
1	Antizichtscherm (100 meter met alle toebehoren), inclusief plaatsen	30	Keer	€ 740
2	Twee informatiewagens inclusief programmeren (informatiewagen dient ook figuren te kunnen weergeven)	30	Keer	€ 450
3	Plaatsen snelheidsbeperkende borden	30	2 stuk	€ 30
4	Twee mobiele lichtmasten / verlichtingswagens	30	Keer	€ 260
5	Veiligstellen/afkoppelen elektrische installaties	60	Keer	€ 250
6	Coördinator Opdrachtnemer (Bijlage C2.7)	45	Uur	Kosten in contract

Vertrouwelijkheid: RWS INFORMATIE

C Ondersteunende veiligheidsmaatregelen / verkeersmaatregelen / personeel				
	Overige / personeel inclusief kosten van transport, gereedschappen en klein materiaal	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
7	Veiligheidsadviseur (Bijlage C2.7)	45	Uur	€ 100
8	Milieudeskundige (Bijlage C2.7)	60	Uur	€ 106
9	Werknemer (algemene medewerker)	45	Uur	€ 52,50
10	Vier verkeersregelaars	45	Uur	€ 210
11	Inzet duikteam (3 personeelsleden)	*(≥180-6 uur)*	Keer (max 4 uur)	€ 900
12	Aanvullende inspectiewerkzaamheden (inspecteur)	45	Uur	€ 150
13	Lasser inclusief las- en brandapparatuur, capaciteit ≥ 10 KVA 230/400 volt	180	Uur	€ 80
14	Monteur E/WTB (ten behoeve van veiligstellen)	45	Uur	€ 110
15	Kostendeskundige opstellen raming ten behoeve van de garant- c.q. borgstelling bij een scheepsaanvaring	45	Uur	€ 120

D Materiaal en Materieel ten behoeve van reparaties en incidentafhandeling op de weg				
Volg nr	**Inzet van materieel inclusief aan- en afvoerkosten**	**Responstijd op locatie na melding in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
1	Omleidingsroute(s) instellen (inclusief U-routes)	30	Keer	€ 1900
2	Het verwijderen van verontreinigingen van en uit het wegdek *(vegen / zuigen / ZOAB-cleanen, gemiddelde oppervlak 20.000 m²)*	30	Keer	€ 1.000
3	Het reinigen van kolken en riolering *(kolkenzuiger)*	30	Keer (max 4 uur)	€ 300
4	Herstellen geleiderailconstructie per calamiteit-/incidentlocatie (gemiddelde lengte 20 m)	90	Keer	€ 1.400
5	Uitwisselen Rimob prestatieklasse 100 R (voor auto(snel)wegen van 100-120 km/uur)	120	St	€ 15.420
6	Uitwisselen Rimob prestatieklasse 110 R (voor auto(snel)wegen van 130 km/uur)	120	St	€ 16.800
7a	Plaatsen (tijdelijk) uitbord BB01 (1500x1800)	60	Keer	€ 250

C Ondersteunende veiligheidsmaatregelen / verkeersmaatregelen / personeel				
	Overige / personeel inclusief kosten van transport, gereedschappen en klein materiaal	**Uiterste responstijd na melding op locatie in minuten**	**Eenheid**	**Prijs per eenheid in euro excl. omzetbelasting**
7b	Plaatsen chevronbord BB03 (1500x3000)	60	Keer	€ 1.750
8	Reparatieploeg asfalt (gaten vullen, scheuren/krassen herstellen)	30	Keer	€ 800
9	Herstellen asfaltschade <25 meter (rijstrook inclusief markering)	240	Keer	€ 6.058
10	Herstellen asfaltschade ≥25 meter en < 50 meter (rijstrook inclusief markering)	240	Keer	€ 7.500
11	Herstellen asfaltschade ≥50 meter en <100 meter (rijstrook inclusief markering)	240	Keer	€ 9.660
12	Hoogwerker *reikwijdte ≥ 13m en werkhoogte ≥ 20m*	60	Keer (max 4 uur)	€ 500
13	Verrichten van betonreparaties aan kunstwerken < 1m^2	60	Keer	€ 430
14	Vrachtauto *met (indien noodzakelijke) hydraulische laad- en losinrichting, inclusief bediening*	60	Uur	€ 95
15	Hydraulische graafmachine *inclusief bediening, inclusief mogelijke hulpmiddelen*	90	Keer (max 4 uur)	€ 352
16	Wiellader *inclusief bediening, inclusief mogelijke hulpmiddelen*	90	Keer (max 4 uur)	€ 217
17	Calamiteitenauto (gereedschap- / materiaalwagen met 220 volt aggregaat, compressor, verlichting, kettingzaag, haspels, onverdunde zoabclean, absorptiekorrels en koud-asfalt, slijptollen (ten behoeve van assistentie Werkzaamheden) inclusief bediening)	90	Keer	€ 250
18	Herstellen van wildrasters en mitigerende maatregelen in alle voorkomende types	120	Keer	€ 350
19	Uitwisselen van een lichtmast inclusief armatuur (tijdelijke mast, geen definitief herstel)	120	Keer	€ 800
20	Vergoeding na vergeefs uitrijden als gevolg van een door de Opdrachtgever gecancelde melding	nvt	Keer	€ 175
E Materiaal en Materieel ten behoeve van reparaties en incidentafhandeling op de vaarweg				

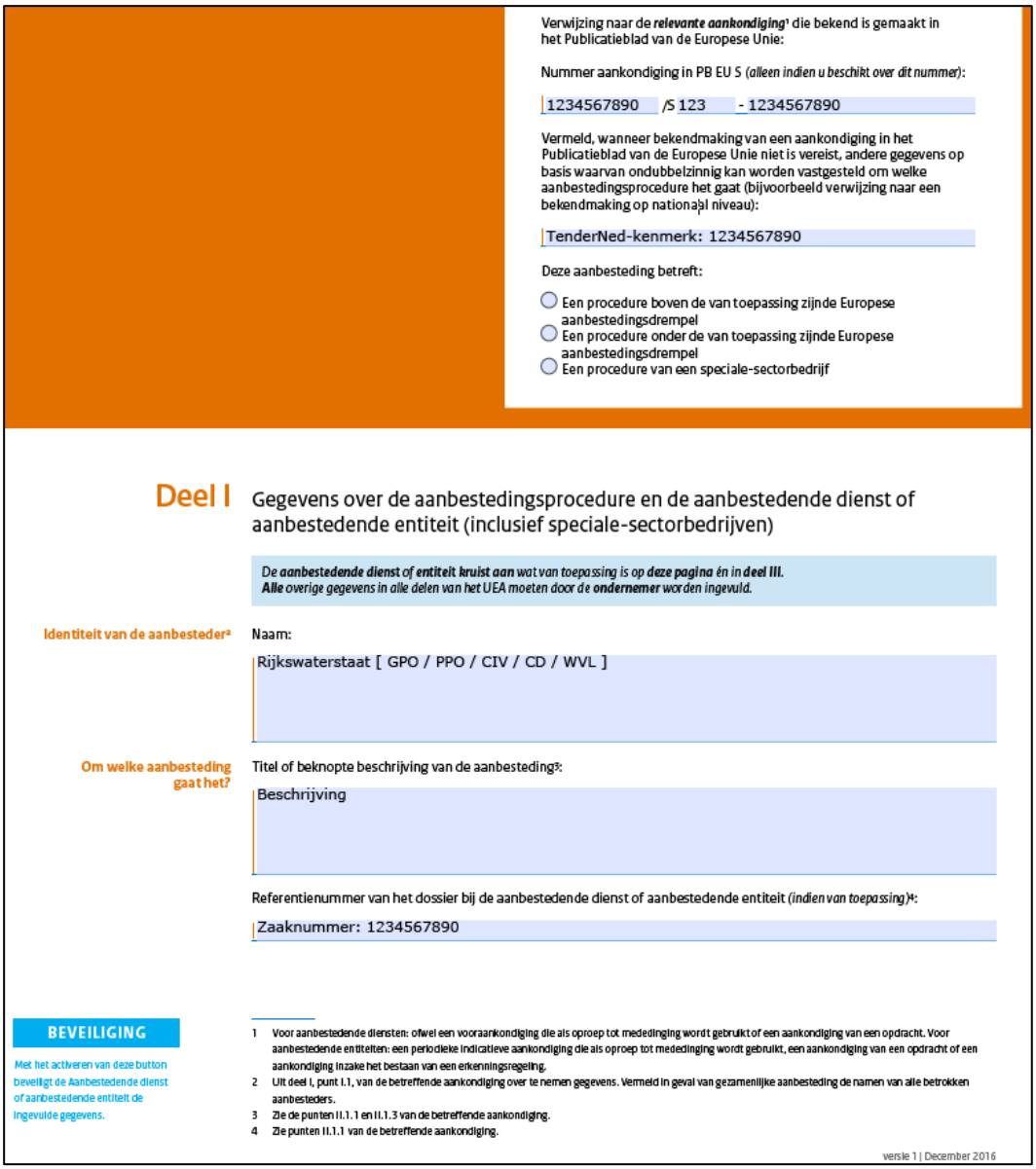
Vertrouwelijkheid: RWS INFORMATIE

Volg nr	Inzet van materieel inclusief aan- en afvoerkosten	Responstijd op locatie na melding in minuten	Eenheid	Prijs per eenheid in euro excl. omzetbelasting
1	Kraanschip met beun *hefvermogen ≥ 20 ton, laadvermogen ≥ 250m3, inclusief bemanning*	180	Uur	€ 400
2	Telekraan *hefvermogen ≥ 100 ton, inclusief bediening*	240	Keer (max 4 uur)	€ 1.050
3	Sleepboot *motorvermogen ≥ 225 kW, inclusief bemanning*	180	Uur	€ 110
4	Sleepboot (motorvlet) *motorvermogen ≥ 100 kW, inclusief bemanning*	180	Uur	€ 106
5	Motorwerkschip met hijscapaciteit *hijscapaciteit ≥ 10.000 kg, inclusief bemanning, motorvermogen 100 kW*	180	Uur	€ 180
6	Zelfvarend kraanponton *hefvermogen ≥ 100 ton, inclusief bemanning*	180	Uur	€ 555
7	Beunschip *800 m3/1280 ton*	180	Uur	€ 550
8	Calamiteitenvaartuig (trailerbaar) met Pick-up inclusief bediening Boot (>20km/h): onzinkbare boot met buitenboordmotor, inclusief trailer, inclusief brandstof en veiligheids- en communicatiemiddelen (marifonie). Bediening inclusief vaarbewijs/marifooncertificaat (2 personen)	90	Uur	€ 450
9	Bergingsvaartuig (varend materieel) *inclusief hefinrichting en las- en brandapparatuur, kraancapaciteit ≥ 40 ton/m, inclusief bemanning*		Uur	€ 950
10	Drijvend ponton met heistelling *hijsvermogen ≥ 40 ton (groot varend materieel)*		Uur	€ 300
11	Generator/aggregaat 150 kVA *met pompen tot 500 m3/uur*		Uur	€ 90
12	Trilblok *vermogen ≥ 261 kW, 230 Nm*		Uur	€ 240
13	Draglineschotten of rijplaten *inclusief plaatsen en verwijderen.* *Benodigd aantal afhankelijk van de situatie*		Keer	€ 200
F Verontreiniging bermen en water				

Volg Nr.	Reinigen / leveren materiaal / stortkosten verontreinigde grond en olie-water sediment	Uiterste responstijd na melding op locatie in minuten	Eenheid	Prijs per eenheid in euro excl. omzetbelasting
1	Berm reinigen (het reinigen van alle mogelijke verontreinigingen op en in de berm)	60	Keer	€ 525
2	Watergang reinigen (het reinigen van alle mogelijke verontreinigingen op en in de watergang) inclusief talud en duikers	60	Keer	€ 720
3	Leveren zand/grond	90	Per m3	€ 25
4	Stortkosten verontreinigde grond < 6 ton inclusief acceptatie en transport (inclusief leveren stortbonnen)	nvt	Keer	€ 465
5	Stortkosten olie-water sediment < 6 ton inclusief acceptatie en transport (inclusief leveren stortbonnen)	nvt	Keer	€ 475
6	Stortkosten verontreinigde grond ≥ 6 ton inclusief acceptatie en transport (inclusief leveren stortbonnen)	nvt	Keer	€ 1.050
7	Stortkosten olie-water sediment ≥ 6 ton inclusief acceptatie en transport (inclusief leveren stortbonnen)	nvt	Keer	€ 925

Vertrouwelijkheid: RWS INFORMATIE

Bijlage S Melding inzet zelfstandige hulppersoon



Verwijzing naar de ***relevante aankondiging***[1] die bekend is gemaakt in het Publicatieblad van de Europese Unie:

Nummer aankondiging in PB EU S *(alleen indien u beschikt over dit nummer)*:

1234567890 /S 123 - 1234567890

Vermeld, wanneer bekendmaking van een aankondiging in het Publicatieblad van de Europese Unie niet is vereist, andere gegevens op basis waarvan ondubbelzinnig kan worden vastgesteld om welke aanbestedingsprocedure het gaat (bijvoorbeeld verwijzing naar een bekendmaking op nationaal niveau):

TenderNed-kenmerk: 1234567890

Deze aanbesteding betreft:

- ○ Een procedure boven de van toepassing zijnde Europese aanbestedingsdrempel
- ○ Een procedure onder de van toepassing zijnde Europese aanbestedingsdrempel
- ○ Een procedure van een speciale-sectorbedrijf

Deel I Gegevens over de aanbestedingsprocedure en de aanbestedende dienst of aanbestedende entiteit (inclusief speciale-sectorbedrijven)

De aanbestedende dienst of entiteit kruist aan *wat van toepassing is op* ***deze pagina*** *én in* ***deel III.***
Alle *overige gegevens in alle delen van het UEA moeten door de* ***ondernemer*** *worden ingevuld.*

Identiteit van de aanbesteder[2]

Naam:

Rijkswaterstaat [GPO / PPO / CIV / CD / WVL]

Om welke aanbesteding gaat het?

Titel of beknopte beschrijving van de aanbesteding[3]:

Beschrijving

Referentienummer van het dossier bij de aanbestedende dienst of aanbestedende entiteit *(indien van toepassing)*[4]:

Zaaknummer: 1234567890

BEVEILIGING

Met het activeren van deze button beveiligt de Aanbestedende dienst of aanbestedende entiteit de ingevulde gegevens.

1 Voor aanbestedende diensten: ofwel een vooraankondiging die als oproep tot mededinging wordt gebruikt of een aankondiging van een opdracht. Voor aanbestedende entiteiten: een periodieke indicatieve aankondiging die als oproep tot mededinging wordt gebruikt, een aankondiging van een opdracht of een aankondiging inzake het bestaan van een erkenningsregeling.
2 Uit deel I, punt I.1, van de betreffende aankondiging over te nemen gegevens. Vermeld in geval van gezamenlijke aanbesteding de namen van alle betrokken aanbesteders.
3 Zie de punten II.1.1 en II.1.3 van de betreffende aankondiging.
4 Zie punten II.1.1 van de betreffende aankondiging.

versie 1 | December 2016

Bijlage T Coördinatie van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen

T.1 Eisen aan coördinatie

T.1.1 Algemeen

1.1.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie te verrichten, zodanig dat het werk en de werkzaamheden van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen worden afgestemd op de Werkzaamheden die voortvloeien uit de Overeenkomst. De Opdrachtnemer dient zorg te dragen dat de Werkzaamheden en het werk en de werkzaamheden van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen op een tijdige, doelmatige, veilige, publieksgerichte en een voor de Opdrachtgever economisch meest verantwoorde wijze worden gerealiseerd en gecommuniceerd.

B-1.1.2 In § T.2 is een overzicht opgenomen van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen.

In lid T.2.1 is een overzicht weergegeven van huidige en voorziene opdrachtnemers en derden, voor zover nu bekend, waarvoor de Opdrachtnemer Werkzaamheden moet verrichten met betrekking tot coördinatie van werken en werkzaamheden.

In lid T.2.2 is een overzicht weergegeven van nevenopdrachtnemers en derden waarvoor Opdrachtnemer, na een verzoek van de Opdrachtgever, tijdelijk Werkzaamheden moet verrichten met betrekking tot coördinatie van werken en werkzaamheden.

In lid T.2.3 is een overzicht weergegeven van voorgeschreven zelfstandige hulppersonen waarvoor de Opdrachtnemer Werkzaamheden moet verrichten met betrekking tot coördinatie van werken en werkzaamheden.

B-1.1.3 De overzichten zoals opgenomen in § T.2 kunnen wijzigen als gevolg van voorgenomen werkzaamheden van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen. De Opdrachtgever zal als gevolg van deze wijzigingen het overzicht actualiseren gedurende de looptijd van de Overeenkomst en dit zo spoedig mogelijk ter kennis brengen van de Opdrachtnemer.

De kosten voortvloeiende uit wijzigingen in de overzichten worden geacht te zijn begrepen in het in artikel 2 lid 5 Basisovereenkomst genoemde totaalbedrag (opdrachtsom).

1.1.4 De Opdrachtnemer dient de Opdrachtgever met bekwame spoed te informeren indien de Opdrachtnemer niet kan voldoen aan de coördinatieverplichting door toedoen van een nevenopdrachtnemer, derde of voorgeschreven zelfstandige hulppersoon.

T.1.2 Opstellen plan coördinatie

1.2.1 De Opdrachtnemer dient een plan voor de coördinatie van werk en werkzaamheden door nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen op te stellen en hieraan invulling te geven, zodanig dat voldaan wordt aan de eisen die voortvloeien uit de Overeenkomst.

1.2.2 De Opdrachtnemer dient in het plan "Coördinatie van werk en werkzaamheden

Vertrouwelijkheid: RWS INFORMATIE

door nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen" ten minste uit te werken:

a. toegang verschaffen tot en begeleiding in het Areaal;
b. coördinatie Veiligheid en Gezondheid (V&G coördinatie);
c. coördinatie duikwerkzaamheden (duikcoördinatie);
d. coördinatie elektrotechnische werkzaamheden;
e. coördinatie cybersecurity werkzaamheden;
f. uit en in bedrijf nemen van installaties of objecten;
g. coördinatie stremmingen, hinder en verkeersmaatregelen;
h. communicatie met beherend, begeleidend en bedienend personeel;
i. opstellen, vaststellen, beheren, communiceren en handhaven van een coördinatieplanning;

T.1.3 Toegang verschaffen en begeleiding in het Areaal

1.3.1 De Opdrachtnemer dient Werkzaamheden te verrichten voor het verschaffen van toegang tot en het begeleiden van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen op objecten en terreinen in het Areaal.

1.3.2 De Opdrachtnemer dient Werkzaamheden te verrichten voor het (in bruikleen) verstrekken en beheren van middelen die toegang geven tot objecten en terreinen in het Areaal.

1.3.3 De Opdrachtnemer dient onbevoegden te gelasten objecten of terreinen c.q. het Areaal te verlaten en zich te vervoegen bij de Opdrachtgever.

B-1.3.4 Medewerkers van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen dienen voor betreding van objecten en terreinen in het Areaal de veiligheidsintroductie van de Opdrachtgever gevolgd te hebben.

1.3.5 De Opdrachtnemer dient nadere objectspecifieke veiligheidsinstructies aan nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen te verzorgen, voorafgaand aan de uitvoering van werkzaamheden door nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen.

T.1.4 Veiligheid en gezondheid

1.4.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot V&G- coördinatie te verrichten zodanig dat, in aanvulling op hetgeen gesteld is in Bijlage K "Integraal Veiligheidsplan" van de Vraagspecificatie, ten minste invulling gegeven wordt aan:

a. het beoordelen van V&G-plannen van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen en de hieruit voortvloeiende bevindingen, voorzien van een advies, ter kennis brengen van de Opdrachtgever;
b. het afstemmen van de V&G-plannen van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen, zodanig dat geen risico's voor veiligheid en gezondheid ontstaan;
c. V&G coördinatiewerkzaamheden over en V&G begeleiding van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen die gelijktijdig (met de Opdrachtnemer) werkzaamheden uitvoeren in het Areaal.

1.4.2 De Opdrachtnemer dient medewerkers van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen die onveilig handelen of een onveilige situatie creëren, te gelasten de onveilige handeling of situatie per direct op te heffen dan wel te staken.
Indien de aanwijzing niet wordt opgevolgd dient de Opdrachtnemer dit direct ter kennis te brengen van de Opdrachtgever.

T.1.5 Duikwerkzaamheden

Vervallen.

T.1.6 Cybersecurity werkzaamheden

1.6.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van cybersecuritywerkzaamheden te verrichten, zodanig dat de ICT- en IA geen verhoogd risico lopen met betrekking tot cybersecurity.

T.1.7 Elektrotechnische werkzaamheden

1.7.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van elektrotechnische werkzaamheden te verrichten, zodanig dat deze op een veilige wijze en conform Bijlage K "Integraal Veiligheidsplan" van de Vraagspecificatie verlopen.

T.1.8 Veiligstellen en uit- en inbedrijfname van objecten en installaties

1.8.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot het veiligstellen en/of de uit- en inbedrijfname van objecten en installaties te verrichten, ten behoeve van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen.

1.8.2 De Opdrachtnemer dient zijn Werkzaamheden met betrekking tot uit -en inbedrijfname van objecten en installaties te verrichten zodanig dat, in aanvulling op Bijlage K "Integraal Veiligheidsplan" van de Vraagspecificatie, ten minste invulling wordt gegeven aan:

a. het beoordelen van uit- en inbedrijfstelprocedures opgesteld door nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen, de hieruit voortvloeiende bevindingen voorzien van een advies, en dit ter kennis brengen van de Opdrachtgever;
b. het gebruik van het formulier conform Bijlage K "Integraal Veiligheidsplan" van de Vraagspecificatie;
c. aanwezigheid van de Opdrachtnemer bij en controle op de daadwerkelijke uit- of inbedrijfname van objecten en installaties.

T.1.9 Stremmingen, hinder en verkeersmaatregelen

1.9.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van stremmingen, hinder en verkeersmaatregelen te verrichten ten behoeve van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen, zodanig dat minimale hinder en maximale veiligheid voor scheepvaart- en wegverkeer wordt gerealiseerd.

1.9.2 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van stremmingen, hinder en verkeersmaatregelen te verrichten conform het Protocol Vaarwegen

T.1.10 Communicatie met beherend, begeleidend en bedienend personeel

1.10.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot communicatie over werkzaamheden met beherend, begeleidend en bedienend personeel van de Opdrachtgever te verrichten, zodanig dat deze te allen tijde hun rol en verantwoordelijkheid kunnen vervullen.

1.10.2 De Opdrachtnemer dient zijn Werkzaamheden met betrekking tot communicatie te verrichten, zodanig dat ten minste invulling wordt gegeven aan:

a. het betrekken van beherend en/of begeleidend personeel tijdens voorbereiding van werkzaamheden en/of Werkzaamheden indien noodzakelijk;
b. het melden aan de ter plaatse bevoegde regioverkeersleider en bedienend personeel van aanwezigheid van medewerkers van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen bij betreding van objecten.

Vertrouwelijkheid: RWS INFORMATIE

1.10.3 Werkzaamheden van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen dienen 1 week voorafgaand aan de werkzaamheden gemeld te worden aan de bevoegde regioverkeersleider door middel van een e-mailbericht.

1.10.4 Werkzaamheden van de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen die het Functioneren of Presteren dan wel de veiligheid van het Areaal beïnvloeden, dienen dagelijks tussen 8.00 en 9.00 uur voorafgaand aan de werkzaamheden gemeld en doorgesproken te worden met de bevoegde regioverkeersleider.

1.10.5 De Opdrachtnemer dient tijdens uitvoering van de werkzaamheden door de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen de communicatie met bedienend personeel en regioverkeersleider te verzorgen.

1.10.6 Alle communicatie voortkomend uit de coördinatieverplichting dient verzorgd te worden door de overallcoördinator als bedoeld in §3.6 (VH040) van de Vraagspecificatie Proces.

T.1.11 Aanvraag en afgifte (werk)vergunningen, ontheffingen, beschikkingen en/of toestemmingen

1.11.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van de aanvraag en afgifte van (werk)vergunningen, ontheffingen, beschikkingen en/of toestemmingen te verrichten zodanig dat de voortgang van de werkzaamheden niet wordt belemmerd.

1.11.2 De Opdrachtnemer dient zijn Werkzaamheden met betrekking tot de coördinatie van aanvraag en afgifte van (werk)vergunningen, ontheffingen, beschikkingen en/of toestemmingen te verrichten zodanig dat ten minste invulling gegeven wordt aan het op verzoek van de Opdrachtgever:

a. beoordelen van de bevoegdheid, juistheid en volledigheid van de aanvraag;
b. verifiëren of de aanvraag conform de coördinatieafspraken is;
c. ter kennis brengen van de Opdrachtgever van de bevindingen met betrekking tot de aanvraag;
d. adviseren van de Opdrachtgever met betrekking tot verlenen van het aangevraagde.

B-1.11.3 De Opdrachtgever is te allen tijde als bevoegde de partij die vergunningen, ontheffingen, beschikkingen en/of toestemmingen afgeeft.

T.1.12 Coördinatieplanning

1.12.1 De Opdrachtnemer dient met betrekking tot de coördinatie van de uitvoering van de werkzaamheden door de Opdrachtnemer, inclusief nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen een coördinatieplanning op te stellen, vast te stellen, te beheren, te communiceren en te handhaven.

1.12.2 De Opdrachtnemer verricht ten behoeve van de coördinatieplanning zoals bedoeld in 1.12.1 de volgende werkzaamheden:

- het inventariseren en actualiseren van de raakvlakken tussen de werkzaamheden van nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen;
- signalering en oplossen van knelpunten ter zake van raakvlakken met nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen;
- het organiseren, voorzitten en notuleren van de benodigde overleggen met nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen.

1.12.3 De Opdrachtnemer dient ieder kwartaal een afschrift van de coördinatieplanning te zenden naar de nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen.

Indien een nevenopdrachtnemer, derde of voorgeschreven zelfstandige hulppersoon bezwaar heeft tegen de coördinatieplanning, dient de Opdrachtnemer zo spoedig mogelijk een overleg te organiseren met betrokkenen.

T.1.13 Controlewerkzaamheden areaalgegevens voor Verkeerscentrale

1.13.1 De Opdrachtnemer dient Werkzaamheden met betrekking tot de coördinatie van revisie van areaalgegevens voor de Verkeerscentrale te verrichten, zodanig dat de Verkeerscentrale over de juiste areaalgegevens beschikt.

B-1.13.2 De nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen leveren de door hen gereviseerde areaalgegevens aan de Opdrachtnemer aan.

1.13.3 De Opdrachtnemer dient binnen 4 weken na ontvangst van de door de nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen gereviseerde areaalgegevens te controleren of deze areaalgegevens voldoen aan de voorschriften van de Verkeerscentrale.

B-1.13.4 De nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen leveren de door hen gereviseerde en door de Opdrachtnemer akkoord bevonden areaalgegevens zelf aan de betreffende gegevensbeheerder van Rijkswaterstaat.

T.2 Overzicht nevenopdrachtnemers, derden en voorgeschreven zelfstandige hulppersonen

T.2.1 Overzicht huidige en voorziene nevenopdrachtnemers en derden

Project/ Contractnr.	**Nevenopdrachtnemer / derde en Werkzaamheden**	**Voorzien tijdstip van uitvoering**	**Vermelding**
Contractnr. 31015991	Ajax Chubb Varel, opdrachtnemer m.b.t. het aanleggen brandblusinstallatie en uitbreiden van bestaande brandmeldinstallatie Oosterscheldekering, inclusief 25 jaar all-in onderhoud	Einddatum: 31-12-2035	
Windpark Krammer BV/contractnummer S-08317	ENERCON Services Netherlands B.V., opdrachtnemer m.b.t. het onderhouden en behouden van de windturbines op een windturbinepark in en op de Philipsdam en Grevelingendam in de gemeente Schouwen-Duiveland	Einddatum onbekend	Opdrachtgever: Windpark Krammer B.V., Rijkswaterstaat heeft zelf geen contract met ENERCON
Contractnummer 31145202	Raamcontractpartners van de raamovereenkomst Civiele Werken in het natte beheersgebied van Rijkswaterstaat Zee en Delta	Einddatum: 14 maart 2023	Raamcontractpartners zijn alleen op het mo-

Vertrouwelijkheid: RWS INFORMATIE

Project/ Contractnr.	Nevenopdrachtnemer / derde en Werkzaamheden	Voorzien tijdstip van uitvoering	Vermelding
			ment dat er een nadere overeenkomst met hen is afgesloten daadwerkelijk in het areaal zijn.
GOVa 7c /Contractnummer 31135639	Witteveen & Bos Raadgevend Ingenieurs B.V., opdrachtnemer m.b.t. contractvoorbereiding en begeleiding realisatiecontract GOVa 7c (remming- en geleidewerken)	Einddatum: 31-12-2021	

T.2.2 Overzicht nevenopdrachtnemers en derden m.b.t. tijdelijke Werkzaamheden

Project / Contractnr.	Nevenopdrachtnemer / derde en Werkzaamheden	Voorzien tijdstip van uitvoering	Vermelding

T.2.3 Overzicht voorgeschreven zelfstandige hulppersonen

Project / Contractnr.	Voorgeschreven zelfstandige hulppersoon en Werkzaamheden	Voorzien tijdstip van uitvoering	Vermelding
31089380	Goudappel Tenuki VOF; doorvoeren wijzigingen aan de verkeerskundige configuratie van de DVM-applicaties.		
31084142	Combinatie Cofely Energy & Infra BV en ARS Traffic & Transport Technology; herstellen dan wel nieuw aanbrengen van een Weigh in Motion (WiM)-systeem.		

Project / Contractnr.	**Voorgeschreven zelfstandige hulp-persoon en Werkzaamheden**	**Voorzien tijd-stip van uitvoering**	**Vermelding**
31079720	Nader door de Opdrachtgever te benoemen zelfstandige hulppersoon; herstellen dan wel nieuw aanbrengen van een gladheid-meldsysteem (GMS).		

Vertrouwelijkheid: RWS INFORMATIE

Bijlage U Informatievoorziening ter plaatse bij verkeersmaatregelen ten behoeve van wegwerkzaamheden

Vervallen.

Bijlage V Richtlijnen Cybersecurity

Inhoud

Deel 1: Cybersecurity Implementatierichtlijn Objecten - RWS

1 Inleiding
- 1.1 Baseline Informatiebeveiliging RWS
- 1.2 Cybersecurity Implementatierichtlijn Objecten – RWS
- 1.3 Instructie voor toepassing
- 1.4 Structuur

2 Specifieke maatregelpakketten
- 2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten
- 2.2 Maatregelen Logische toegang
- 2.3 Maatregelen Beveiligingsincidenten en incident Response Plan
- 2.4 Maatregelen Netwerkkoppelingen
- 2.5 Maatregelen bescherming tegen malware, hardening en patching
- 2.6 Maatregelen Logging en Monitoring
- 2.7 Maatregelen Bewustwording en Training
- 2.8 Maatregelen gecontroleerd wijzigen
- 2.9 Maatregelen beheer en onderhoud
- 2.10 Maatregelen Back-ups

Bijlage A: Wachtwoord Richtlijn
Bijlage B: Factsheet Wachtwoorden
Bijlage C: Begrippen

Deel 2: Bijlagen: Richtlijnen Cybersecurity

Inleiding
CS R01 - Richtlijn omgaan met vertrouwelijke informatie en documenten
CS R02 - Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS
CS R03 - Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging
CS R04 - Richtlijn continuiteitsplan
CS R05 - Richtlijn camera's en omgang met camerabeelden van de verkeersregistratiesystemen
CS R06 - Richtlijn registratie CI items in een configuration management database

Deel 3: Template Plan Cybersecurity

1. Inleiding
   - 1.1 Doel
   - 1.2 Scope
2. Risico's
   - 2.1 Risico's
3. Cybersecurity beheersmaatregelen
   - 3.1 Comply or explain
   - 3.2 Risico's
   - 3.3 Beheersmaatregelen
     - 3.3.1 Belegging verantwoordelijkheden
     - 3.3.2 Borging Cybersecurity
     - 3.3.3 Onderaannemers

Vertrouwelijkheid: RWS INFORMATIE

3.3.4 Beheer bedrijfsmiddelen, CMDB
3.3.5 Aanvaardbaar gebruik toegangsmiddelen
3.3.6 Classificatie en beveiliging informatie
3.3.7 Bewustwording, scholing en VOG
3.3.8 Fysieke toegangsbeveiliging
3.3.9 Logische toegangsbeveiliging tot ICT en IA-systemen
3.3.10 Wachtwoordrichtlijn
3.3.11 Back-up en recovery proces
3.3.12 Beveiliging documentatie
3.3.13 Wijzigingsproces
3.3.14 Beveiliging tegen malware, hardening en patching
3.3.15 Patch proces en kritieke Patches
3.3.16 Koppeling van apparatuur
3.3.17 Logging en monitoring
3.3.18 Datanetwerkkoppelingen
3.3.19 Remote Access
3.3.20 Gebruik veilige communicatieprotocollen
3.3.21 Webapplicaties
3.3.22 Continuïteit en herstel dienstverlening
3.3.23 Testen continuïteitsplannen
3.3.24 Beveiliging Spionage
3.3.25 Beveiliging van de Informatievoorziening
3.3.26 Cybersecurity inbreuken en verhoogde dreiging
3.3.27 Security gerelateerde wijzigingen
4. Jaarlijkse toestandsrapportage cybersecurity
4.1 Bevindingen
4.2 Analyse cybersecurity incidenten
4.3 Testresultaten back-up en recovery proces
4.4 Testresultaten continuiteitsplannen en -voorzieningen
4.5 Risicoanalyse en risicoafweging

Deel 1: Cybersecurity Implementatierichtijn Objecten – RWS

Cybersecurity

Implementatiericht-lijn

Objecten – RWS

Uitgegeven door	PRIA / CIV-IRN Security Center
Steller	Turabi Yildirim
Datum	04 augustus 2015
Status	Definitief
Vertrouwelijkheid	RWS informatief
Informatieklasse	RWS-0
Versie	1.4

1. Inleiding

Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en Industriële Automatisering. Hiermee wordt bijgedragen aan de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatievoorziening (IV) en de Industriele Automatisering (IA) van RWS.

1.1 Baseline Informatiebeveiliging RWS

De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor. De BIR biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van het Rijk. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.
In het beveiligingsbeleid van IenM wordt de Baseline Informatiebeveiliging Rijksdienst (BIR) gehanteerd als het te volgen Tactisch Normen Kader voor de beveiliging van de IV. De BIR is daarmee ook kaderstellend voor RWS. De BIR hoofdstukken en paragrafen worden integraal aangehouden voor de vertaalslag en invulling van de beveiliging van de IV van RWS. De Baseline Informatiebeveiliging RWS (BIR RWS) is het resultaat van de vertaalslag en invulling van de BIR voor de beveiliging van de IV van RWS.

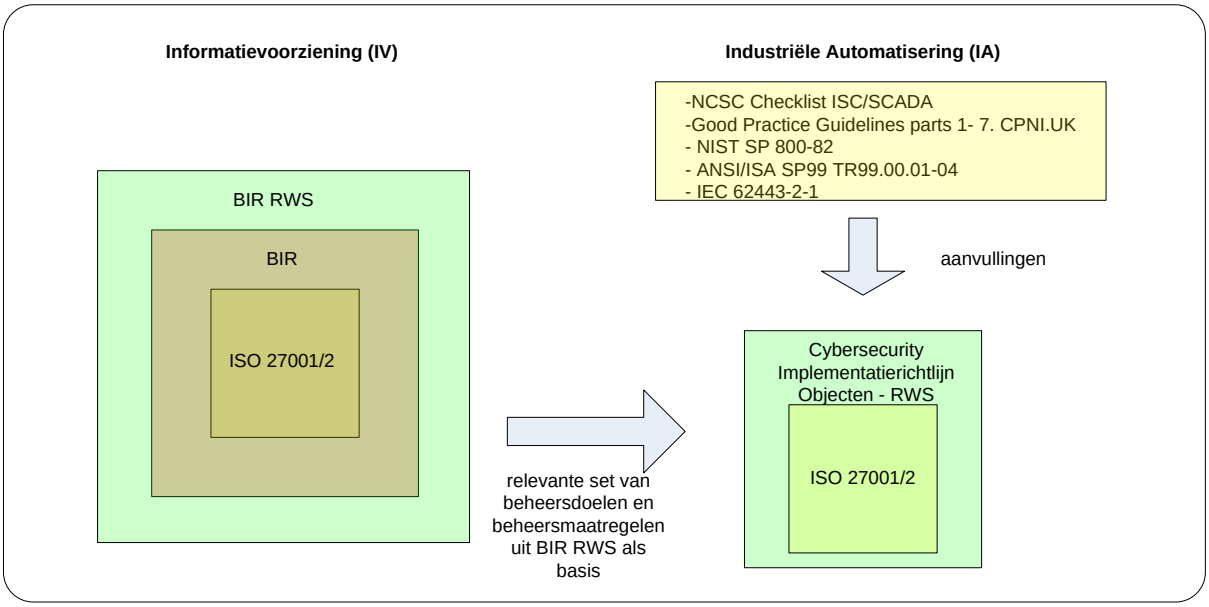
1.2 Cybersecurity Implementatierichtlijn Objecten – RWS

RWS heeft veel systemen en omgevingen die los staan van de centrale kantooromgeving. Dit zijn veelal operationele systemen voor het bedienen van objecten, het communiceren met vaarweggebruikers of het modelleren van waterkwaliteit en -kwantiteit in verschillende stroomgebieden. Deze systemen hebben vaak een ander dreigingprofiel dan de IV in de kantooromgeving en staan daar vaak ook los van zoals de Industriële Automatisering (IA) met veel ICS/SCADA-toepassingen.

Hiernaast heeft RWS ook op grote schaal te maken met uitbesteding van werk en het voeren van regie op de uitbestede taken aan marktpartijen. Bij deze samenwerking en uitvoering van werkzaamheden door marktpartijen speelt (IA) en inzet van ICS/SCADA-systemen een grote rol. De BIR (RWS) is voor de IA omgeving en de ICS/SCADA toepassingen niet volledig dekkend en op onderdelen te algemeen van aard waardoor bedrijfsrisico’s blijven bestaan voor RWS.

Het Beveiligingsbeleid van IenM geeft aan dat de dienstonderdelen daar waar nodig aanvullingen dienen te plegen op de BIR om de beveiligingsrisico’s in het eigen werkveld te mitigeren. De uitvoeringstaken van RWS waarbij de inzet nodig is van IA en vele ICS/SCADA-systemen, zijn van dien aard dat extra eisen en maatregelen naast de BIR (RWS) noodzakelijk zijn.

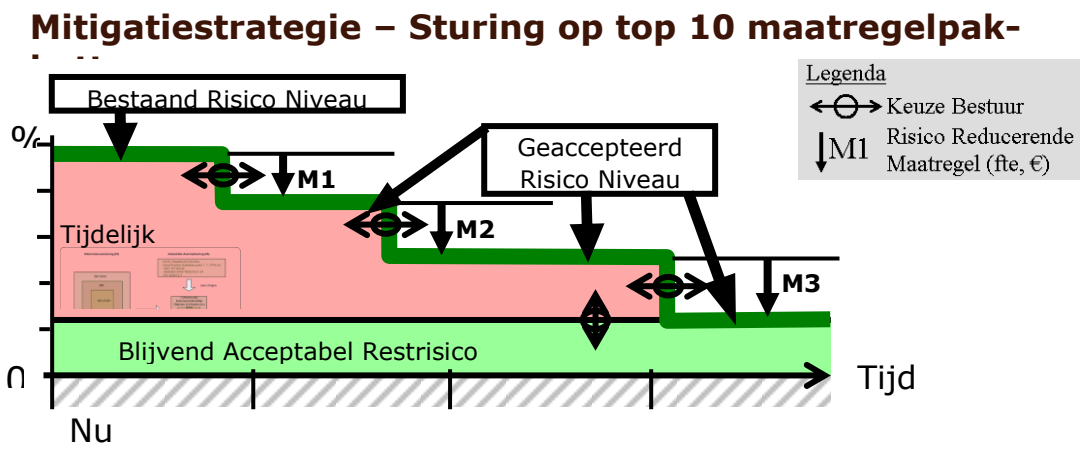
Afhankelijk van het domein, het karakter van de samenwerking, de uitbesteding van taken en de operationele behoefte neemt RWS binnen de kaders van het beveiligingsbeleid van IenM de ruimte om afgeleide implementatierichtlijnen uit de BIR RWS te ontwikkelen en van toepassing te verklaren zoals de Cybersecurity Implementatierichtlijn Objecten - RWS. Schematisch ziet dit er als volgt uit:



De Cybersecurity Implementatierichtlijn Objecten - RWS is een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR RWS en de NCSC Checklist beveiliging ICS/SCADA systemen voor de beveiliging van objecten RWS. Waar nodig zijn aanvullingen gedaan uit good practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen. De formulering van de beheersdoelen en beheersmaatregelen heeft meer een operationeel karakter en is daardoor geschikt voor zowel RWS interne doelgroepen zoals objectbeheerders en projecten als voor gebruik bij inkooptrajecten, contracten, vraagspecificaties en uitvoering van werk door marktpartijen.

Tevens is in de Cybersecurity Implementatierichtlijn Objecten - RWS rekening gehouden met de risico mitigatiestrategie van RWS. Op basis van interne en externe onderzoeksrapporten en de hieruit voortvloeiende aanbevelingen is er voor gekozen om te starten met een set van top 10 maatregelpakketten. Bij implementatie van deze maatregelen zal RWS/Opdrachtnemer de belangrijkste kwetsbaarheden die kunnen leiden tot een onacceptabel risico voor RWS op het vlak van functionaliteit, veiligheid en imagoschade gaan beheersen. Primair hebben de maatregelen het doel om misbruik, uitval en fouten binnen de IV en IA te voorkomen.

Verder is in de richtlijn gezocht naar een balans tussen de meer generieke beheersdoelen en beheersmaatregelen uit de BIR RWS en de meer specifieke beheersdoelen en beheersmaatregelen op basis van de risico's en de risicogestuurde aanpak binnen RWS voor het werkveld van de IA.



Vertrouwelijkheid: RWS INFORMATIE

1.3 Instructie voor toepassing

RWS streeft naar een passend niveau van beveiliging voor de objecten en de Infrastructuur waar de objecten onderdeel van uitmaken. Daarbij wordt aan een object een specifieke cyber-classificatie toegekend (zie voor deze cyber-classificatie per object de meest recente versie van de Infraclassificatie[1]). Deze cyber-classificatie correspondeert met een zgn. cybersecurity-weerstandsniveau, conform onderstaande tabel.

Classificatie object in Infraclassificatie	**Cybersecurity weerstandsniveau**
A	4
B	3
C	2
D	1
E	1

Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3. In dit document is een implementatierichtlijn opgenomen per weerstandsniveau.

Cybersecurity weerstandsvermogen in Ketens: Elke keten is zo sterk als de zwakste schakel. Indien de bediening of het beheer van object A wordt gedaan vanuit een initieel lager geclassificeerd object B, wordt de classificatie van dat object B verhoogd tot het cybersecurity weerstandsniveau van object A.
Als een RWS object nog niet voorzien is van een cyber-classificatie dient er contact gezocht te worden met de afdeling Security Center van RWS-CIV-IRN voor advies en correcte indeling qua cybersecurity weerstandsniveau.
In het geval dat er helemaal geen object uit de infraclassificatie lijst objecten voorkomt in de scope van de overeengekomen dienstverlening dan dient voor de beveiliging van de ICT-, ICS/SCADA-, DVM-systemen en datanetwerkcomponenten binnen de Infrastructuur RWS het Cybersecurity weerstandniveau van 1 te worden aangehouden.

Voorbeeld
Uitgaande van een tunnel met cyber-classificatie B (volgens bovenstaande vertaaltabel) dienen alle Cybersecurity beveiligingseisen zoals beschreven bij de proces- en systeem eisen in het contract, uitgewerkt te worden in het beveiligingsplan van de Opdrachtnemer. Voor de tunnel dienen de Cybersecurity beveiligingseisen uit het contract aangevuld te worden met maatregelen uit de bindende bijlagen waarnaar wordt verwezen in de proces- en systeemeisen. Bij de aanvulling met maatregelen dient voor de tunnel conform de bovenstaande vertaaltabel het cybersecurity weerstandsniveau 3 aangehouden te worden. Bij mogelijke overlap tussen de Cybersecurity proces- en systeemeisen in het contract en de specifiekere maatregelen uit de maatregelpakketten, dienen de specifieke maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens invulling gegeven aan de Cybersecurity proces- en systeemeisen in het contract.

1.4 Structuur

In het contract zijn de relevante beheersdoelen (lees Cybersecurity beveiligingseisen) en beheersmaatregelen beschreven die afgeleid zijn uit de BIR (RWS). Naast de Cybersecurity beveiligingseisen uit de BIR RWS zijn tevens de relevante Cybersecurity beveiligingseisen en beheersmaatregelen uit de NCSC Checklist beveiliging

[1] Momenteel op te vragen bij PRIA of CIV-IRN/Security Center

ICS/SCADA systemen opgenomen in het contract. Indien noodzakelijk worden vanuit de proces- en systeemeisen verwezen naar de maatregelpakketten waar een verdieping plaatsvindt in de maatregelenset en dit is weer afhankelijk van het risico en het cybersecurity weerstandsniveau dat gehaald moet worden.

Hoofdstuk 2 beschrijft de maatregelpakketten die een verdieping of aanvulling vormen op de Cybersecurity beveiligingseisen. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS hanteert. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS. Afhankelijk van de infraclassificatie en de daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maatregelpakketten is gebruik gemaakt van de NCSC Checklist beveiliging ICS/SCADA systemen en overige good practices voor de beveiliging van IA en ICS/SCADA systemen.

In bijlage A en B zijn de wachtwoord richtlijn en de Factsheet Wachtwoorden opgenomen.

Vertrouwelijkheid: RWS INFORMATIE

2 Specifieke maatregelpakketten

De specifieke maatregelpakketten zijn een aanvulling en verdieping op de Cybersecurity beveiligingseisen en maatregelen zoals beschreven bij de proces- en systeemeisen in het contract. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS volgt om tot beheersing van kwetsbaarheden te komen. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS.

RWS streeft naar een passend niveau van beveiliging voor de objecten. Daarbij wordt aan een objecttype een zgn. Cybersecurity weerstandsniveau toegekend dat correspondeert met het te beschermen belang van het object. Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3.

In de tabel hieronder wordt het Cybersecurity weerstandsniveau weergegeven dat nagestreefd moet worden voor de beveiliging van de verschillende objecten.

Cyber classificatie object in Infraclassificatie	**Cybersecurity weerstandsniveau**
A	4
B	3
C	2
D	1
E	1

Afhankelijk van de infraclassificatie en het daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven.

Bij mogelijke overlap tussen de Cybersecurity proces- en systeemeisen in het contract en de specifiekere maatregelen uit de maatregelpakketten, dienen de specifieke maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens invulling gegeven aan de Cybersecurity proces- en systeemeisen in het contract.

2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten

Cybersecurity Weerstandsniveau	**4**	**3**	**2**	**1**
VRKI-referentie	4	3	2	1
Toegangsbeheer	Rijkspas VG-IA	Rijkspas Kantoor	Sleutel	Sleutel
Toegangsproces	Lokaal geldende regels en processen			
Organisatorisch	O2	O2	O1	O1
Bouwkundig	B3	B2	B1	B1
Compartimentering	C/M3	C/M2	C/M1	C/M1
Inbraak-installatie	E3	E2	E1	E1
Alarmering	AL3	AL2	AL1	AL0
Alarm opvolging	R3	R2	R1	R0

N.B.:

1. Naast bovengenoemde weerstandsniveaus 1 t/m 4 zijn door de DG en politieke top specifieke maatregelenpakketten te definiëren. Hierbij valt bijvoorbeeld te denken aan bomvrije ruimten, kogelvrij glas of 24-uur on-site bewaking.
2. Voor richtlijnen voor de integrale fysieke beveiliging wordt verwezen naar het Handboek Security RWS (GPO).
3. Gemotiveerd afwijken van de hier genoemde implementatierichtlijnen kan, bijv. als dat efficiënter is in de integrale aanpak, als maar wel aan de bovenliggende weerstandseisen wordt voldaan.

Toelichting tabellen

Toegangsbeheer
Rijkspas VG-IA Toegang middels Rijkspas Vitale Gebieden (vanuit IA-perspectief) installatienormen (Grade 3)
Rijkspas Kantoor Toegang middels Rijkspas Kantoor installatienormen
Sleutel Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)

Toegangsproces
Uitgangspunt is dat alleen toegang wordt verleend aan personen (internen / externen incl. bezoekers) die in de IA-gerelateerde ruimten moeten zijn vanwege het verrichten van werkzaamheden of het houden van toezicht.

Organisatorische maatregelen

O1 Standaard maatregelen + voorlichting over preventie + uitleg over het systeem.
O2 Als O1 + specifieke maatregelen opnemen in beveiligingsplan.

Bouwkundige maatregelen
B0 Het aanwezige hang- en sluitwerk handhaven.
B1 Hang- en sluitwerk met een inbraakwerendheid van 3 minuten volgens BRL3104 of klasse 2 NEN5096.
B2 Idem met inbraakwerendheid van 5 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.
B3 Idem met inbraakwerendheid van 10 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.

Compartimentering / Meeneem beperkende maatregelen

Vertrouwelijkheid: RWS INFORMATIE

C/M1 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M1 door verankeren, verplaatsen. Of bouwkundig compartiment C1. Alles met inbraakvertraging van 3 minuten.
C/M2 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M2 door slagvaste vitrines, rolluiken e.d. Of bouwkundig compartiment C2. Alles met inbraakvertraging van 5 minuten.
C/M3 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M3 door mistgenerator. Of bouwkundig compartiment C3. Alles met inbraakvertraging van 10 minuten.

Elektronische maatregelen
Ed Alleen voor woningen in risicoklasse 1. De (domestic) alarminstallatie met mogelijke doormelding naar (mobiele) telefoon. Grade 2 /NCP 2
E1 Inbraakalarminstallatie. Grade 2 /NCP 2
E2 Inbraakalarminstallatie met ruimtelijk werkende anti-masking detectoren. Grade 2 / NCP 2
E3 Inbraakalarminstallatie met anti-masking detectoren. Componenten Grade 3 /NCP 3

Alarmering
AL0 Optische en/of akoestische alarmgever en/ of alarmtransmissie naar (mobiele) telefoon
AL1 Alarmtransmissiesysteem niveau AL1 volgens NEN EN 50136-1-1 naar een PAC.
AL2 Alarmtransmissiesysteem niveau AL2 volgens NEN EN 50136-1-2 naar een PAC.
AL3 AL2 aangevuld met back-up melding (AL1) via andere transmissieweg (GPRS) naar de PAC.

Reactie (alarmopvolging)
R0 Alarmopvolging door sleutelhouder na melding naar (mobiele) telefoon.
R1 Alarmopvolging door PAC naar de sleutelhouder(s).
R2 Alarmopvolging door PAC naar een erkende Particuliere Bewakingsdienst.
R3 Als R2 + Politie (prioriteit 1) Technische alarmverificatie verplicht.

2.2 Maatregelen Logische toegang

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	LTM 1	LTPO 1 t/m 5, 8, 9 en 10	LTT 1 t/m 3
3	LTM 1	LTPO 1 t/m 5, 7, 9	LTT 1 t/m 3
2	LTM 1	LTPO 1 t/m 6 en 9	LTT 1 t/m 3
1	LTM 1	LTPO 1 t/m 6 en 9	LTT 1 t/m 3

Mens	LTM1	Voor bewustwording, gedragsregels en training van, bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training"
Procedures & Organisatie	LTPO1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.
	LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend op basis van het 'need to have' principe plaatsvindt; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het noodzakelijke; • fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan wordt voor personen die hiertoe geautoriseerd zijn; • bij misbruik van accounts en autorisaties dienen disciplinaire maatregelen te worden genomen.
	LTPO3	De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dient jaarlijks beoordeelt en geactualiseerd te worden in een formeel proces.
	LTPO4	De lokale logische toegang voor medewerkers tot de RWS infrastructuur, ICT, ICS/SCADA systemen en de centrale en lokale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager aangevraagd en goedgekeurd te worden.
	LTPO5	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die RWS hiervoor beschikbaar stelt.
	LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – minimaal een user-id en wachtwoord combinatie met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO7	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – 'two-factor' authenticatie ('bezit' plus 'kennis') met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO8	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – Rijkspas Vitaal ('bezit' plus 'kennis') met navolging van de wachtwoordricht-

Vertrouwelijkheid: RWS INFORMATIE

		lijn (indien technisch nog niet mogelijk dan minimaal op basis van user-id en wachtwoord combinatie) • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS/CIV.
	LTPO9	Er dient een geborgde procedure te bestaan die de toewijzing en verspreiding van authenticatiemiddelen aan bedienaars, beheerders en overig ondersteunend personeel regelt alsmede het innemen daarvan bij functiewisseling of vertrek (in-, door- en uitstroming). In deze procedure dient ook de voorgeschreven handelingen bij verlies, diefstal dan wel beschadiging te worden opgenomen.
	LTPO10	De toegang voor onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van dat onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en teruggezet bij afmelding van de call.
Techniek	LTT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.
	LTT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.
	LTT3	Voor bedienaars en beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

2.3 Maatregelen Beveiligingsincidenten en incident Response Plan

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	BIRM1	BIRPO1 t/m 7	BIRPT1
3	BIRM1	BIRPO1 t/m 7	BIRPT1
2	BIRM1	BIRPO1 t/m 3, 5 en 6	BIRPT1
1	BIRM1	BIRPO1 t/m 3 en 5	BIRPT1

Mens	BIRPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen security incidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen moet worden geëist dat zij alle security incidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.
	BIRPO2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.
	BIRPO3	Er is bestaat een geborgde procedure voor de reactie op en eventuele escalatie van security incidenten. De security incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de bedienaars, beheerders en overig onder-

		steunend personeel zowel van RWS als die van externe partijen.
	BIRPO4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op die van RWS-CIV.
	BIRPO5	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incident-manager van RWS-CIV ingeschakeld.
	BIRPO6	Er dient een geborgde procedure te bestaan voor incident-respons ingeval van incidenten en calamiteiten.
	BIRPO7	Jaarlijks dienen de incident responseplannen beproefd te worden aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van incidentresponse is het testen van de noodbediening.
Techniek	BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

2.4 Maatregelen Netwerkkoppelingen

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	NKM 1	NKPO 1 t/m 8	NKT 1 en 2
3	NKM 1	NKPO 1 t/m 8	NKT 1 en 2
2	NKM 1	NKPO 1, 2, 4, 5, 6 en 8	NKT 1 en 2
1	NKM 1	NKPO 1, 2, 4, 5, 6 en 8	NKT 1 en 2

Mens	NKM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	NKPO1	De Opdrachtnemer draagt zorg voor en ziet erop toe dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van RWS (zoals vastgelegd in de PDC Netwerken van RWS- CIV) en dat de overige generieke centrale netwerkdiensten evenals overige ondersteunende ICT worden afgestemd en afgenomen van de RWS dienst Centrale Informatievoorziening (CIV). Rechtstreekse toegang tot ICS/SCADA-systemen vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail - is verboden.
	NKPO2	De Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen het object en de centrale netwerken van RWS (NNV/VicNet) de aansluitvoorwaarden van NNV/VicNet in acht worden genomen. Voor remote logische toegang van personeel tot de aan het object gekoppelde systemen moet de procedure "Toegang Derden" van RWS-CIV worden gevolgd waarbij de Objectverantwoordelijke/-beheer de aanvraag verzorgt.
	NKPO3	De Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met de RWS-CIV voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de RWS Netwerkarchitectuur inclusief security en de IA-kaderstelling.
	NKPO4	De Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen tussen ICS/SCADA systemen en andere datanetwerken beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm

Vertrouwelijkheid: RWS INFORMATIE

		van beveiliging kent en geen onacceptabele risico's oplevert voor het object en de centrale netwerkdienstverlening. Voor elke koppeling is een risicoanalyse en afweging gemaakt.
	NKPO5	De Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen malware, hardening en patching').
	NKPO6	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van de Opdrachtnemer.
	NKPO7	De Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door middel van een Configuration Management Database (CMDB).
	NKPO8	De Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit RWS-CIV.
Techniek	NKT1	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
	NKT2	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.

2.5 Maatregelen bescherming tegen malware, hardening en patching

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	MHPM 1	MHPPO 1 t/m 10	MHPT 1 t/m 2
3	MHPM 1	MHPPO 1 t/m 10	MHPT 1 t/m 2
2	MHPM 1	MHPPO 1 t/m 5, 8, en 10	MHPT 1 t/m 2
1	MHPM 1	MHPPO 1 t/m 5, 8, en 10	MHPT 1 t/m 2

Mens	MHPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	MHPPO1	De Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware waarbij de anti-malware software en signature updates dagelijks dienen plaats te vinden.
	MHPPO2	De Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen door: • niet noodzakelijke datanetwerkservices uit te zetten; • het verwijderen (patchen) van bekende kwetsbaarheden; • alle poorten die niet nodig zijn te deactiveren/blokkeren; • alle default "access points" te verwijderen;

		• De default accounts uit te schakelen conform het wachtwoord policy; • Indien beschikbaar gebruik te maken van de security opties van leveranciers.
	MHPPO3	De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.
	MHPPO4	De Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
	MHPPO5	De Opdrachtnemer dient over een geborgde procedure te beschikken voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden.
	MHPPO6	Bij patches en anti-virusupdates, die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.
	MHPPO7	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging schriftelijk te worden vastgelegd voorzien van een risicoafweging.
	MHPPO8	De Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
	MHPPO9	Voor zover technisch te scannen dienen zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te worden gescand.
	MHPPO10	De Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op malware gecontroleerd worden voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
Techniek	MHPT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.
	MHPT2	Antimalware voorzieningen moeten in afstemming met RWS-CIV ingezet worden.

2.6 Maatregelen Logging en Monitoring

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	LMM1	LMPO1 t/m 5	LMT1 t/m 5
3	LMM1	LMPO1 t/m 5	LMT1 t/m 5
2	LMM1	LMPO1 t/m 4	LMT1 t/m 4
1	LMM1	LMPO1 t/m 4	LMT1 t/m 4

Mens	LMM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures	LMPO1	De handelingen van medewerkers, beheerders, meldingen

Vertrouwelijkheid: RWS INFORMATIE

& Organisatie		vanuit systemen en eventlogs dienen te worden vastgelegd in audit-logbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf; • een tot een natuurlijk persoon herleidbare gebruikersnaam of een (systeem)-ID • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis • optioneel de identiteit van het werkstation of de locatie • een doorlopende en unieke nummering per logregel
	LMPO2	De Opdrachtnemer draagt zorg voor en ziet er op toe dat: • de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden drie maanden bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
	LMPO3	Voor de levering van logbestanden aan derden dient de RWS Objectverantwoordelijke/-beheerder expliciet toestemming te verlenen.
	LMPO4	De Opdrachtnemer draagt zorg voor een geborgde procedure die opvolging geeft aan meldingen uit de centrale logging en monitoringsvoorzieningen en proces vanuit RWS-CIV.
	LMPO5	De Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het ICS/SCADA en gekoppelde ICT-componenten in kaart gebracht. Een geborgde procedure is aanwezig voor het bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.
Techniek	LMT1	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en- netwerkelementen dienen in CSV-formaat opgeleverd te kunnen worden.
	LMT2	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.
	LMT3	Het overschrijven of verwijderen van logregels- en bestanden wordt gelogd in een nieuw aangelegde log.
	LMT4	De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.
	LMT5	Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen moet in afstemming met en op verzoek van Opdrachtgever beveiligingsspecifieke logsystemen worden ingezet.

2.7 Maatregelen Bewustwording en Training

Niveau	**Medewerker**	**Manager**
4	BTME1 t/m 22	BTMA1 t/m 6
3	BTME1 t/m 22	BTMA1 t/m 6
2	BTME1 t/m 22	BTMA1, 2, 3, 5 en 6
1	BTME1 t/m 22	BTMA1, 2, 5 en 6

Medewerker	BTME1	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door Opdrachtgever aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen.
	BTME2	Iedere medewerker is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.
	BTME3	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
	BTME4	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.
	BTME5	Bij het constateren van een security incident dient de Opdrachtnemer, bedienaar, beheerder en overig ondersteunend personeel dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het Cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: • verlies van dienst, apparatuur of voorzieningen; • systeemstoringen of overbelasting; • menselijke fouten die leiden tot functionele verstoring of uitval van systemen; • inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; • inbreuk op de bediening en beheer; • ongeautoriseerde systeemwijzingen; • niet-naleving van beleid of gedragsregels; • virusmeldingen; • verlies of diefstal van bedrijfsmiddelen; • oneigenlijk gebruik van bevoegdheden; • - vandalisme, moedwillige beschadiging.
	BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.
	BTME7	De Opdrachtnemer, Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
	BTME8	Bedienaars, beheerders en overig ondersteunend perso-

Vertrouwelijkheid: RWS INFORMATIE

		neel gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangsmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
	BTME9	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
	BTME10	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.
	BTME11	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.
	BTME12	Voor de Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
	BTME13	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
	BTME14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.
	BTME15	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieksaccounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van RWS.
	BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient de Opdrachtnemer dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
	BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
	BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.
	BTME19	Gegevensdragers worden altijd vooraf op malware gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
	BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME21	Onregelmatigheden, incidenten en storingen binnen het

		back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME22	De Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.
Manager	BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt door de Opdrachtnemer en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
	BTMA2	De Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: • de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel, objectverantwoordelijke/-beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; • ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; • dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen alle bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van RWS die ze in hun bezit hebben retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; • dat de toegangsrechten van alle bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.
	BTMA3	De Opdrachtnemer/objectverantwoordelijke/-beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.
	BTMA4	De Opdrachtnemer ziet erop toe dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging zoals fysieke en logische toegang en melding van beveiligingsincidenten. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steekproefsgewijze controles vastgesteld en uitgevoerd.
	BTMA5	De Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en be-

Vertrouwelijkheid: RWS INFORMATIE

		heerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
	BTMA6	De Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.

2.8 Maatregelen gecontroleerd wijzigen

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	GWM 1	GWPO 1 t/m 9	GWT 1 en 2
3	GWM 1	GWPO 1 t/m 9	GWT 1 en 2
2	GWM 1	GWPO 1 t/m 3, 5, 7 en 9	GWT 1 en 2
1	GWM 1	GWPO 1 t/m 3, 5, 7 en 9	GWT 1 en 2

Mens	GWM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	GWPO1	De Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) inventariseren en registreren van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden.
	GWPO2	De Opdrachtnemer dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.
	GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.
	GWPO4	Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen dient altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten voordat uitvoering van werkzaamheden plaatsvindt zijn goedgekeurd door de Objectverantwoordelijke/ -beheerder.
	GWPO5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.
	GWPO6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten indien mogelijk vooraf aan de implementatie in productie te worden getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit of beveiliging van de organisatie. Indien haalbaar moet voor ICS/SCADA en overige ondersteunende ICT-systemen controle worden uitgevoerd voor de authenticiteit/integriteit van de software voorafgaande aan de implementatie op operationele systemen.
	GWPO7	De Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebrachte als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.
	GWPO8	Voor elke wijziging is een terugval scenario opgesteld

		waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. Kort na de implementatie van een wijziging dient een test plaats te vinden om te verifiëren dat de wijziging is gelukt of dat op het terugval scenario moet worden overgegaan.
	GWPO9	De Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.
Techniek	GWT1	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.
	GWT2	Voor zover beschikbaar wordt gebruik gemaakt van test-voorzieningen.

2.9 Maatregelen beheer en onderhoud

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	BOM 1	BOPO 1 t/m 8	BOT 1 t/m 2
3	BOM 1	BOPO 1 t/m 8	BOT 1 t/m 2
2	BOM 1	BOPO 1 t/m 4, 6 en 8	BOT 1 t/m 2
1	BOM 1	BOPO 1 t/m 4, 6	BOT 1 t/m 2

Mens	BOM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BOPO1	De Opdrachtnemer draagt zorg voor het evalueren van risico's en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cyclemanagement.
	BOPO2	De Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer- en onderhoudscontracten met zelfstandige hulppersonen: • Geheimhouding opgenomen is; • Training- en opleidingsvereisten alsmede overige benodigde certificeringen beschreven zijn; • Welke screening van personeel nodig is (bijv. VOG); • Beschreven is dat de RWS gedragsregels voor beveiliging en communicatie strikt in acht moeten worden genomen; • Een concrete procedure bekend is en is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) • De procedures voor fysieke toegang tot objecten en ruimten en de logische toegang tot systemen vastgelegd zijn; • De registratie en rapportage van beveiligingsincidenten geregeld is; • Beschreven is dat handelingen van medewerkers en systemen gelogd en gemonitord worden; • Beschreven is dat loggegevens van RWS beschermd moeten worden tegen verlies en wijziging en niet voor andere doeleinden gebruikt mogen worden; • De bewaartermijnen van back-ups en logbestanden geregeld is; • De procedures voor aan- en afkoppeling van apparatuur beschreven zijn; • De netwerkaansluitvoorwaarden overeengekomen zijn; • De procedure "Toegang Derden" van de CIV gevolgd moet worden voor de logische toegang tot netwerken en systemen. De tijdelijke toegang tot de systemen ten

Vertrouwelijkheid: RWS INFORMATIE

		behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. • Beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die voorzien zijn van de laatste security updates en patches en actuele viruscontroleprogrammatuur; • Beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van RWS verlopen; • Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van RWS; • Beschreven is dat wijzigingen conform het wijzigingsproces van RWS uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden van RWS uitgevoerd moeten worden; • Beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; • Beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het RWS of objectnetwerken strikt verboden is.
	BOPO3	De Opdrachtnemer draagt waar nodig zorg voor en ziet erop toe dat in de SLA/DAP afspraken met Opdrachtgever en zelfstandige hulppersonen worden gemaakt over: • De dienstverlening en functionaliteit; • Tijd van openstelling, bereikbaarheid en reactietijd, incident melding en afhandeling; • Wat wordt verstaan onder een storing, beveiligingsincident en zwakke plek; • Het classificeren van incidenten en de geldende maximale oplossingsduur; • Escalatieprocedures (horizontaal en verticaal) bij overschrijding van de overeengekomen normtijden inclusief namen en telefoonnummers. • Het indienen en afhandelen van wijzigingsverzoeken; • Directe melding van beveiligingsincidenten; • Noodprocedures met zowel interne als externe leveranciers voor ICT en ICS/SCADA systemen; • Ondersteuning bij calamiteiten en beschikbaarheid van reserve onderdelen en apparatuur; • De communicatielijnen (wie, wanneer en waarover); • Hoe de fysieke en logische toegang tot systemen en ruimten geregeld is; • De bewaartermijn van back-ups en logbestanden; • Rapportages die verplicht zijn zoals die voor beveiligingsincidenten en welke frequentie daarvoor geldt; • Het signaleren van nieuwe kwetsbaarheden en tijdig uitbrengen van patches door de leverancier; • Het testen van software-updates alvorens deze in productie gaan; • Evaluatie en actualisatie;
	BOPO4	De Opdrachtnemer draagt zorg voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICT en IA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
	BOPO5	De Opdrachtnemer draagt zorg voor een geborgde procedure die de personele toegang van al het vast onderhoudspersoneel voorafgaand de uitvoering van werkzaamheden regelt. Hiervoor kan de onderstaande "Good Practice" "**Maat-**

		regelen personele toegang" gebruikt worden.
	BOPO6	De Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: • de uitvoering van wijzigingen conform de wijzigingen procedure; • de procedure voor fysieke toegang; • de procedure voor logische toegang; • patching, de back-up procedure en bewaartermijnen; • incidentmanagement, log- en incidentrapportages en de analyse hiervan.
	BOPO7	De Opdrachtnemer draagt zorg voor en ziet erop toe dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.
	BOPO8	De Opdrachtnemer dient jaarlijks de opzet, bestaan en werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever.
Techniek	BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.
	BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV.

Good Practice - Maatregelen personele toegang

De Opdrachtnemer dient te verzorgen dat al het vast onderhoudspersoneel voorafgaand aan zijn/haar operationele inzet en vervolgens steeds binnen een periode van twee jaar:
- een persoonlijke geheimhoudingsverklaring ondertekent en overhandigt aan de Opdrachtgever;
- zich daarbij legitimeert en een goed gelijkende pasfoto overhandigt aan de Opdrachtgever;
- een Verklaring Omtrent Gedrag (VOG) bezit en een kopie daarvan aan de Opdrachtgever overlegt welke is gerelateerd aan de beoogde Werkzaamheden.

Hangende de aanvraag voor een VOG kan volstaan worden met een eigen verklaring van de betreffende medewerker gedurende een periode van maximaal zes weken welke niet verlengd kan worden.
De Opdrachtnemer dient er op toe te zien dat al het onderhoudspersoneel dat niet structureel verschijnt:
- Zich legitimeert;
- In specifieke gevallen op eerste verzoek van de Opdrachtgever bereid is een eigen verklaring en een geheimhoudingsovereenkomst te ondertekenen.

De Opdrachtnemer dient al haar medewerkers nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.
Iedere geconstateerde afwijking van bovenstaande eisen dient door de Opdrachtnemer te worden behandeld als security incident.

2.10 Maatregelen Back-ups

Niveau	**Mens**	**Procedures & Organisatie**	**Techniek**
4	BUM 1	BUPO 1 t/m 5	BUT 1

Vertrouwelijkheid: RWS INFORMATIE

3	BUM 1	BUPO 1 t/m 5	BUT 1
2	BUM 1	BUPO 1 t/m 5	BUT 1
1	BUM 1	BUPO 1 t/m 3	BUT 1

Mens	BUM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van de Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BUPO1	Dagelijks dient automatisch een back-up gemaakt te worden van alle in het systeem aanwezige dynamische en configuratiegegevens welke back-up op het systeem zelf of op de hoofdlocatie van het systeem mag worden opgeslagen. De juiste verwerking van de back-up wordt bewaakt op basis van het back-up log. Deze back-ups worden een week bewaard.
	BUPO2	De integriteit en beschikbaarheid van de laatste drie versies van de ICS/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: • systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd, met deze back-up moet men in staat zijn een volledige rollback naar de werkende situatie terug te kunnen gaan; • Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevind; • Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; • Back-ups worden bewaard tot het moment van uitdienstname van betreffend systeem; • Ingeval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.
	BUPO3	Er bestaan gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.
	BUPO4	Herstelprocedures moeten jaarlijks worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd. Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is. Herstelprocedures zijn onderdeel van de disaster recovery planning.
	BUPO5	Door de Opdrachtnemer worden maandelijks de gemelde incidenten en storingsmeldingen inzake back-up geëvalueerd en waar nodig maatregelen getroffen.
Techniek	BUT1	Benodigde voorzieningen voor het back-up en restoreproces worden in overleg met de Opdrachtgever ingevuld.

Bijlage A: Wachtwoord Richtlijn

Er is een wachtwoordbeleid geïmplementeerd voor de ICS/SCADA systemen die het achterhalen van wachtwoorden economisch onrendabel en praktisch onhaalbaar maakt. Eindgebruikers en beheerders leven dit wachtwoordbeleid na. De "factsheet wachtwoorden" maakt integraal onderdeel uit van de Wachtwoord Richtlijn.

De eisen aan een wachtwoord zijn als volgt:

- Lengte: wachtwoorden bestaan minimaal uit 8 karakters voor gebruikers en minimaal 15 karakters voor beheerders;
- Sterkte: wachtwoorden moeten minimaal bestaan uit een combinatie van cijfers, hoofd- en kleine letters en leestekens;
- Hergebruik van hetzelfde wachtwoord op vervangingsmomenten is niet toegestaan;
- De standaard/default account en wachtwoord wordt uitgeschakeld of na eerste gebruik tijdens installatie gewijzigd;
- Na de initiële installatie van een IA- of ICT-component mag er geen default account/wachtwoordcombinaties meer aanwezig zijn in de component.

Voor de hieronder genoemde accounttypen dient de standaard fabrieksaccount met bijbehorend wachtwoord altijd gewijzigd te worden door een persoonlijk account en wachtwoord. Tevens dient voor de onderkende accounttypen de aangegeven duur voor wachtwoordvervanging alsmede de wachtwoordlengte aangehouden te worden. Bij (legacy) systemen en procestoepassingen waar dit niet mogelijk is, moet een risico-inschatting worden gemaakt en compenserende maatregelen worden getroffen. De afwijkingen worden gedocumenteerd.
De voorschriften rondom accounts en wachtwoorden voor kantoorautomatiseringstoepassingen zijn ter verkrijgen bij de afdeling IV - Security Center van RWS-CIV.

Onderkend worden de volgende typen accounts voor ICS/SCADA met bijbehorende eisen:
Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT-producten van fabrikanten worden gewijzigd.

Alle accounts dienen in een onderstaande **account-type** te worden ingedeeld en te voldoen aan de eisen die aan het betreffende type account gesteld worden:

SCADA-Operatoraccount
Een persoonlijk account dat wordt gebruikt voor de bediening van SCADA systemen
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: min. 15 karakters

SCADA-applicatiebeheeraccount
Een persoonlijk account dat wordt gebruikt om de applicatie op het SCADA systemen te beheren
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 30 dagen
Wachtwoordlengte: min. 15 karakters

SCADA-Systeemaccount (service/applicatie account)
Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten.
Soort: service
Wachtwoord vervanging: 365 dagen
Wachtwoordlengte: min. 15 karakters

Vertrouwelijkheid: RWS INFORMATIE

SCADA-Administratoraccount
Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 30 dagen
Wachtwoordlengte: min. 15 karakters

Kantoorautomatiseringsaccount (KA-account)
Het persoonlijke gebruikers account waarmee men kan werken op de Rijkswaterstaat Kantoorautomatiseringsomgeving.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: min. 8 karakters

Bijlage B: Factsheet Wachtwoorden

Factsheet wachtwoorden voor gebruikers van IA systemen

Aanleiding
Steeds meer Industriële Automatiseringssystemen worden aan andere computersystemen of netwerken gekoppeld. Daarmee neemt de kans toe dat deze systemen vanaf een andere computer of netwerk worden gehackt, met mogelijk verstrekkende gevolgen.
Door het handhaven van fabriekswachtwoorden of eenvoudig te kraken wachtwoorden op IA systemen kunnen kunstwerken en verkeerssystemen relatief eenvoudig worden overgenomen door hackers, als ze via internet of fysiek toegang kunnen krijgen tot de IA systemen.

Toepassing factsheet
In deze factsheet zijn de richtlijnen opgenomen, die binnen Rijkswaterstaat gelden voor het gebruik en wijzigen van sterke wachtwoorden in IA systemen. Ook zijn richtlijnen opgenomen hoe de wachtwoorden moeten worden beschermd.

De richtlijnen zijn niet altijd implementeerbaar in bestaande IA systemen. Als dit het geval is moet een risicoanalyse worden gemaakt door de systeemeigenaar en moeten aanvullende maatregelen worden getroffen om risico's tot een aanvaardbaar niveau terug te brengen. Bijlage 1 geeft door middel van een risico reductie overzicht aan met welke risico's rekening is gehouden in de richtlijn en welke maatregelen daartegen moeten worden getroffen.

Checklist eigenschappen sterke wachtwoorden
1. een wachtwoord moet uit minimaal 15 karakters bestaan
2. een wachtwoord moet minimaal drie van de volgende 5 soorten karakters bevatten:
a. gewone letters
b. hoofdletters
c. getallen
d. punctuatie (bijvoorbeeld: ";'?,!)
e. speciale karakters (bijvoorbeeld: @#$%^&*<>~+=)
3. het default account en wachtwoord van de applicatie mogen niet worden gehandhaafd en moeten beiden bij ingebruikname van de applicatie direct worden gewijzigd en verwijderd.

Zwakke wachtwoorden hebben de volgende eigenschappen:
- het wachtwoord bevat minder dan 15 karakters (en kan door een hacker binnen enkele uren worden gekraakt door willekeurige karakters uit te proberen)
- het wachtwoord is terug te vinden in een woordenboek (en kan door een hacker makkelijk worden geraden met behulp van een woordenboekaanval)
- het wachtwoord is voor de gebruiker makkelijk te bedenken (en voor de hacker dus makkelijk te raden):
  a. namen van familieleden, huisdieren, vrienden, collega's, stripfiguren, etc.
  b. computer namen en -termen, commando's, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd
  c. woorden als "Rijkswaterstaat"; Amaliasluis, Rotterdam, etc.
  d. geboortedata en andere persoonlijke informatie als adres en telefoonnummers
  e. één van de voorafgaande woorden, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.)
- het default account/wachtwoord is nog steeds in gebruik (en de hacker kent die ook of kan het eenvoudig opzoeken op internet of in de handleiding)

Tips voor het maken en onthouden van sterke wachtwoorden
- maak een wachtwoord dat is gebaseerd op een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (Bijvoorbeeld: Het rijmpje "Als het regent in mei is april

Vertrouwelijkheid: RWS INFORMATIE

voorbij en leggen alle vogels een ei" wordt "Ahri5i4velavee", waarbij de maanden zijn vervangen door cijfers)
- maak een zin (passphrase) in plaats van een wachtwoord (password). Typ de woorden van een makkelijke zin achterelkaar en vervang woorden of letters door hoofdletters, getallen of lettertekens (Bijvoorbeeld: 03KleineKleutertjesdiezatenopeen###).

Checklist wachtwoordbescherming
1. Gebruik voor je bedrijfs-account niet hetzelfde wachtwoord als voor je privéaccounts (bijvoorbeeld: persoonlijke gmail, facebook, ANWB site, bol.com, etc.).
2. Gebruik binnen het bedrijf niet overal hetzelfde wachtwoord. Gebruik een verschillend wachtwoord voor je gewone desktopomgeving, je bedienplek of je yammer account.
3. Deel je wachtwoord met niemand, tenzij dit is vereist volgens de procedures.
4. Wachtwoorden mogen nooit worden opgeschreven of digitaal worden opgeslagen zonder te zijn vercijferd.
5. Schrijf nooit een wachtwoord in e-mail, chat of ander communicatiemiddel.
6. Praat niet over je wachtwoord, geef geen hints over je wachtwoord aan anderen.

Slechte opslag van wachtwoorden voldoet aan de volgende eigenschappen:
- Het wachtwoord is opgeschreven en ligt binnen handbereik (en de hacker die fysiek binnendringt, kan het wachtwoord ook gemakkelijk vinden).
- Het wachtwoord van 15 karakters is opgeslagen in een applicatie dat is beveiligd met 8 karakters (en daarmee is de wachtwoordlengte gereduceerd tot 8 karakters, want nu hoeft de hacker alleen nog een wachtwoord van 8 karakters te kraken om bij het wachtwoord van 15 karakters te komen).
- Het wachtwoord is opgeslagen in een document op een gezamenlijke schijf of op sharepoint (en de hacker kan het op afstand of ter plaatse ook vinden. Op afstand heeft hij alle tijd om rustig op zoek te gaan).

Tips voor het opslaan van wachtwoorden
- Als het niet anders kan en wachtwoorden moeten toch worden opgeslagen (bijvoorbeeld, omdat dat volgens een veiligheidsprocedure moet), sla een wachtwoord dan op in een fysieke kluis of een speciaal daarvoor ontwikkelde beveiligde applicatie.
- Als een wachtwoord in een kluis wordt opgeslagen, zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.
- Als een wachtwoord in een beveiligde applicatie wordt opgeslagen, dan is er vaak weer een wachtwoord nodig om die applicatie te openen. Daarvoor geldt wederom de wachtwoordrichtlijn.

Checklist wachtwoordwijziging
1. Wachtwoorden moeten regelmatig worden gewijzigd, met een frequentie die is voorgeschreven in de wachtwoordrichtlijn (in de bijlage staat de wachtwoordrichtijn van mei 2013. Op intranet is steeds de meest recente richtlijn te vinden).

Tips voor het wijzigen van wachtwoorden
- Als het afdwingen van wijzigen van wachtwoorden niet automatisch wordt afgedwongen, zorg dan dat het procedureel wordt afgedwongen. Dit kan simpelweg door zelf (bijvoorbeeld op de eerste maandag van de maand) het wachtwoord te wijzigen.

Checklist locken bedien- of beheerstation
1. Als bedienaars of beheerders een bedien- of beheerruimte langere tijd geheel verlaten, dienen zij het bedien- of beheerstation af te sluiten.
2. Als bedienaars of beheerders een bedien- of beheerruimte korte tijd geheel verlaten, dienen zijn het bedien- of beheerstation te locken.

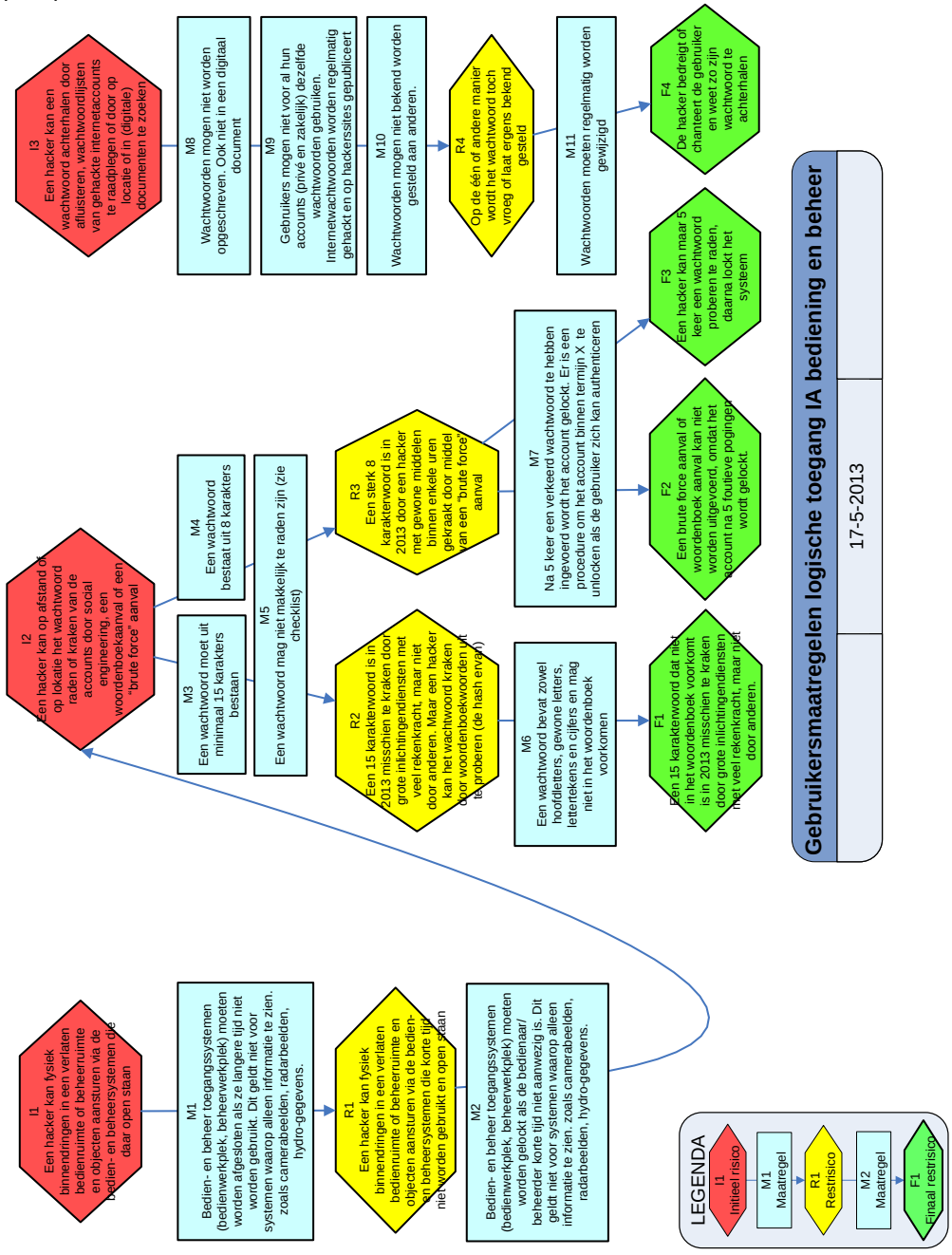
Tips voor het locken van bedien- of beheerstation

- Het is niet nodig om terminals af te sluiten waarop alleen informatie te zien is als camerabeelden of radarbeelden. Het gaat er om dat een onbevoegde geen toegang heeft tot bediening- en beheeromgevingen.
- In sommige situaties mogen of kunnen bedienstations niet worden afgesloten, omdat daardoor juist onacceptabele risico's worden geïntroduceerd. In overleg met de beheerder moet dan worden afgesproken en vastgelegd op welke wijze wordt voorkomen dat onbevoegden toegang krijgen tot de bedien- of beheerruimte als die korte of lange tijd geheel wordt verlaten.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage 1 Gebruikersmaatregelen

Risicoreductieoverzicht logische toegang IA bediening en beheer vanuit gebruikers-perspectief



Bijlage C: Begrippen

Cybersecurity
Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en Industriële Automatisering.

Informatievoorziening (IV)
Het geheel aan hulpmiddelen (waaronder ICT en IA), gegevensverzamelingen en organisatorische inrichtingen, dat dient tot het verstrekken van informatie.

Industriële Automatisering (IA)
Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Dit omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen).

Informatie- en Communicatietechnologie (ICT)
Informatie- en Communicatietechnologie omvat een samenhangend geheel van informatiesystemen, hardware en software, operating systemen van servers, de onderliggende technische datanetwerkinfrastructuur met datanetwerken en bijbehorende datanetwerkcomponenten, dataopslag in rekencentrum, computer- en technische ruimten met als doel het mogelijk maken of ondersteunen van de processen.
Industrial Control Systems (ICS)
Industrial Control Systems zijn systemen die toegerust zijn voor de bediening en besturing van de RWS Infrastructuur waarbij ook gebruik wordt gemaakt van SCADA systemen.

Supervisory Control And Data Acquisition (SCADA)
SCADA systemen verzamelen, verwerken en visualiseren meet- en regelsignalen.

RWS Infrastructuur
RWS infrastructuur staat voor de netwerkinfrastructuur (het Areaal) van RWS: de wegen, vaarwegen en watersystemen.

Vertrouwelijkheid: RWS INFORMATIE

Deel 2: Bijlagen Richtlijnen Cybersecurity

Colofon

Uitgegeven door	RWS – CIV/IRN – Security Centre
Informatie	
Telefoon	
Fax	
Uitgevoerd door	
Opmaak	
Datum	4-8-2015
Versienummer	1.1

Inleiding

In dit document Bijlagen Richtlijnen Cybersecurity zijn als bijlagen de documenten opgenomen waarnaar vanuit contractteksten verwezen wordt. Het zijn op zichzelf staande documenten waar apart naar verwezen kan worden.

Vertrouwelijkheid: RWS INFORMATIE

CS R01 - Richtlijn omgaan met vertrouwelijke informatie en documenten

Medewerkers van Rijkswaterstaat en haar opdrachtnemers moeten op de juiste wijze omgaan met vertrouwelijke informatie (documenten en gegevens). Dit is mede van groot belang voor de beveiliging van de ICT infrastructuur en de primaire processen van Rijkswaterstaat tegen cyber- criminaliteit. Beveiliging van de informatievoorziening en bedienketens in het primair proces, hangt direct samen met de beveiliging van de documentatie betreffende de ICT-infrastructuur.

De vertrouwelijkheid van informatie wordt uitgedrukt in een classificatie. Het classificeren van informatie wordt steeds meer een standaard onderdeel van de professionele werkwijze van alle Rijkswaterstaters. De classificatie geeft de aard van de informatie weer en helpt de gebruiker bij het bepalen hoe het document verwerkt moet (of mag) worden. De volgende informatie classificatie houdt Rijkswaterstaat aan:

RWS Ongeclassificeerd
Deze informatie is voor iedereen toegankelijk.

RWS Bedrijfsinformatie
Deze informatie is alleen toegankelijk voor diegenen die het nodig hebben om hun werkzaamheden uit te kunnen voeren. Hiervoor wordt de regel 'need-to-know' gehanteerd. Dit principe houdt in dat alleen aan die medewerkers toegang wordt verleent omdat zij het nodig hebben voor de uitvoering van hun werkzaamheden.

Departementaal Vertrouwelijk
Deze informatie dient strikt vertrouwelijk te worden behandeld en mag allen op basis van 'need-to-know' verstrekt worden. Deze informatie uitwisseling valt buiten de scope voor informatie uitwisseling met opdrachtnemers.

De projectdocumenten die tussen Rijkswaterstaat en een Opdrachtnemer uitgewisseld worden hebben als hoogste classificatie: RWS Bedrijfsinformatie. In de overeenkomst tussen Rijkswaterstaat en een Opdrachtnemer zijn eisen opgenomen voor geheimhouding en het vertrouwelijk omgaan met documenten. Voorbeelden, gerelateerd aan cybersecurity, van RWS Bedrijfsinformatie zijn:

- ontwerpdocumenten, constructietekeningen en -berekeningen;
- bediening en beheer handleidingen, veiligheidsinstructies en documentatie;
- configuratiedocumentatie van ICT en ICS/SCADA-systemen;
- datanetwerkschema's en IP adressen;
- informatie over de ligging van kabels en leidingen;
- informatie over accounts en wachtwoorden.

Hieronder volgen de maatregelen voor opslag, uitwisseling en verwerking van documenten die de classificatie RWS Bedrijfsinformatie hebben:

- RWS Bedrijfsinformatie is alleen op basis van het 'need-to-know' principe toegankelijk voor de medewerkers van Rijkswaterstaat en de Opdrachtnemer;
- Rijkswaterstaat en de Opdrachtnemer zijn vanaf het moment van ontvangst van informatie verantwoordelijk om binnen de eigen organisatie de ontsluiting en verwerking van de informatie op de afgesproken werkwijze van 'need-to-know' te verzorgen;

- Geprinte exemplaren van verwerkingen van RWS Bedrijfsinformatie dienen in afgesloten kasten bewaard te worden. Bij digitale opslag in de eigen kantoor-omgeving is versleuteling niet verplicht;

- De uitwisseling van RWS Bedrijfsinformatie mag via de mail onvercijferd tussen Rijkswaterstaat en de Opdrachtnemer plaatsvinden. De maximale bestands-grootte van de mailbijlagen bij RWS is 25 MB;

- Grotere bestanden mogen uitgewisseld worden via de IenM Wetransfer (van Ministerie van Infrastructuur en Milieu) of de gewone variant van Wetransfer, mits de documenten eerst worden versleuteld (encrypten) conform bijlage A: Gebruik van 7-Zip voor versleuteling en voorzien van een sterk wachtwoord. Een sterk wachtwoord bestaat uit minimaal 8 karakters, bevat minimaal één hoofdletter, één cijfer en één symbool (bijvoorbeeld !, #, & of @) en is of bevat geen volledig woord of een naam. Het wachtwoord mag niet via het zelfde communicatiekanaal worden uitgewisseld als de bestanden. Geadviseerd wordt om na ontvangst van het versleutelde bestand bij het uitpakken deze bestanden weer zonder wachtwoord op te slaan in de eigen verwerkingsomgeving;

- Het wachtwoord wordt via de contactpersonen tussen Rijkswaterstaat en de Opdrachtnemer uitgewisseld. Het overeengekomen wachtwoord wordt via SMS of telefonisch tussen Rijkswaterstaat en de Opdrachtnemer uitgewisseld en één keer per kwartaal ververst. De contactpersonen delen het wachtwoord op basis van het ‘need-to-know’ principe verder met de betrokken medewerkers binnen de eigen organisatie.

Bijlage A bij CS R01
Gebruik van 7-Zip voor versleuteling

Over 7-ZIP

7-ZIP is een computerprogramma om bestanden te archiveren en comprimeren. Met 7-ZIP kun je echter niet alleen bestanden "inpakken", maar ook versleutelen, ook wel encryptie genoemd. Hiermee zorg je ervoor dat de bestanden uitsluitend kunnen worden geopend door personen die in bezit zijn van de bijbehorende unieke sleutel en/of het wachtwoord en daarmee is 7-ZIP ook een hulpmiddel voor het werken met vertrouwelijke informatie.

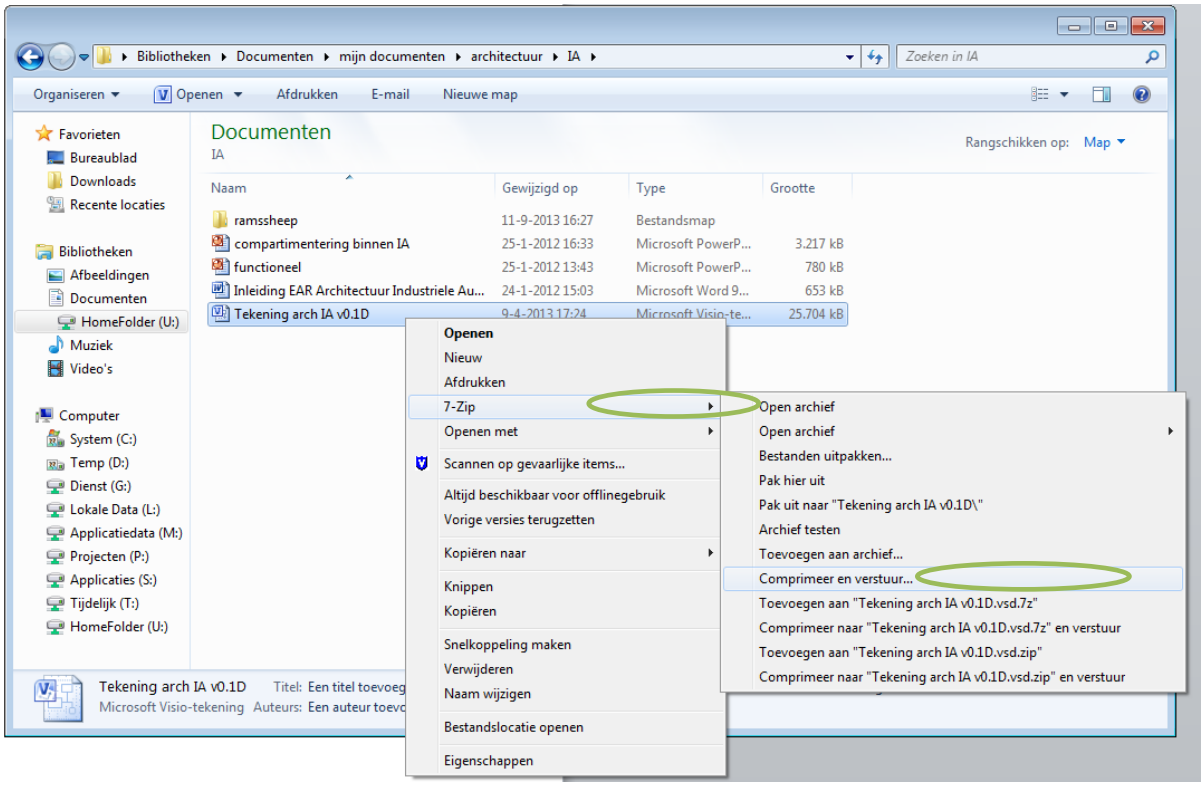
Er zijn meerdere (gratis) programma's om bestanden in te pakken en van een wachtwoord te voorzien, maar 7-ZIP heeft een vrij sterke encryptiemethode, is standaard aanwezig op de RWS Werkplek en is tevens gratis voor (thuis)gebruik. (zie http://www.7-zip.org/).

Deze instructie laat zien hoe je een document rechtstreeks vanuit Windows Verkenner versleuteld kunt mailen.

Documenten versleuteld mailen

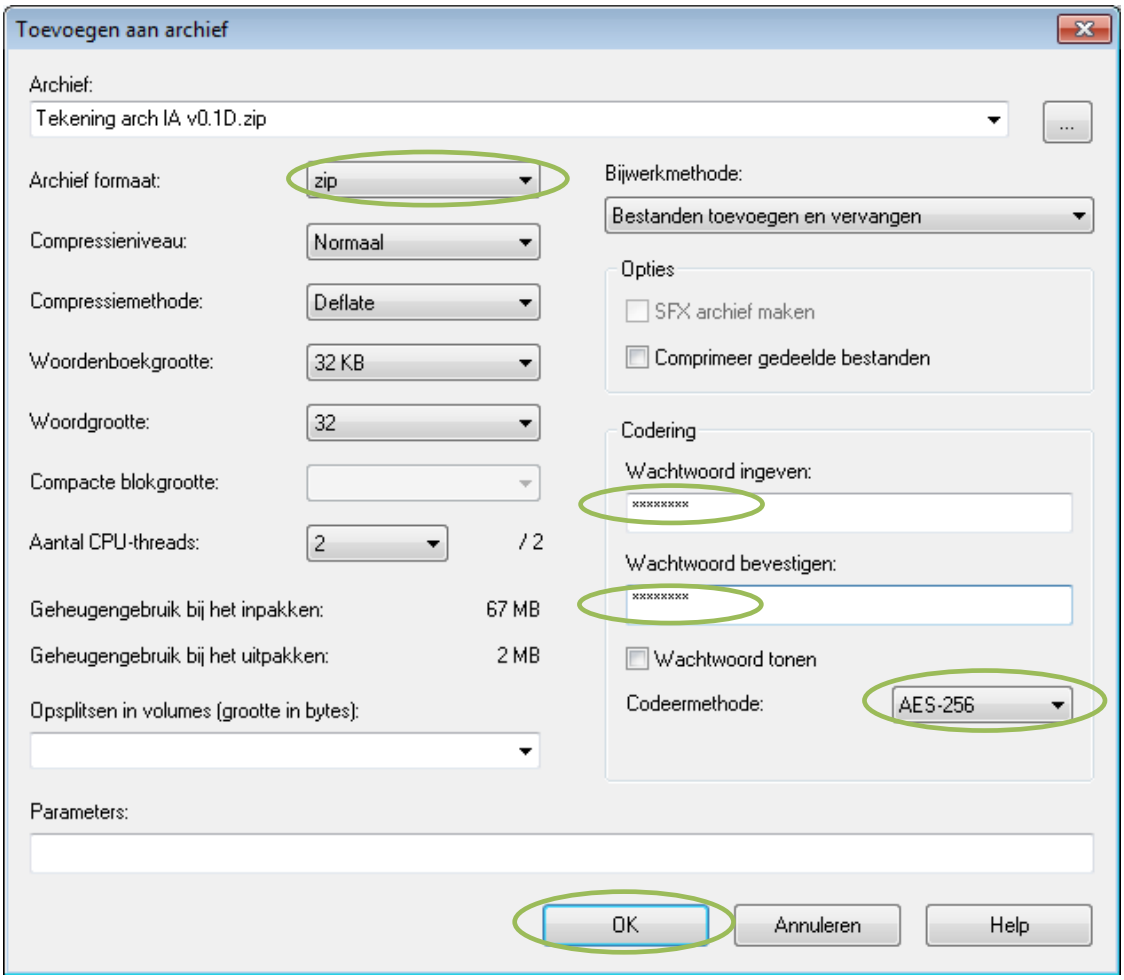
1. Ga naar de Windows verkenner en klik met de rechtermuisknop op het bestand dat je wilt versturen.

2. Kies in het keuzemenu dat verschijnt vervolgens voor: 7-zip[2] -> Comprimeer en Verstuur…



Het volgende scherm verschijnt:

[2] Zichtbaar na installatie van 7-zip.



1. Kies je favoriete archief formaat (ZIP is de meest gangbare);
2. Vul bij "Wachtwoord ingeven" een sterk[3] wachtwoord in, en bevestig deze. NB: het is extreem belangrijk om een sterk wachtwoord te kiezen, hiermee valt of staat het nut van encryptie;
3. Kies bij Codeermethode voor AES-256 (dit is de meest sterke codeer-optie);
4. Klik vervolgens op OK.

De zip-file wordt aangemaakt en direct als bijlage in een leeg mailbericht geplaatst. Het versleutelde bestand is daarmee klaar om verstuurd te worden.

Geef vervolgens het bijbehorende wachtwoord door aan de ontvangende partij. Dat kan telefonisch, mondeling of per SMS, maar niet via internet (e-mail, WhatsApp) waarover ook het versleutelde bestand is verzonden.

Een praktische werklijn is om losse bestanden eerst in een moederbestand te bundelen conform onderstaande instructie. Daarna hoeft alleen maar het moederstand versleuteld te worden.

1. Inpakken van bestanden en/of mappen naar een 'moeder'bestand.

Je kunt meerdere bestanden of een volledige map (inclusief diens bestanden en sub-mappen) makkelijk in één keer samenvoegen.
Stap 0.

[3] Een sterk wachtwoord bestaat uit minimaal 8 karakters, bevat minimaal één hoofdletter, één cijfer en één symbool (bijvoorbeeld !, #, & of @) en is of bevat geen volledig woord of een naam.

Vertrouwelijkheid: RWS INFORMATIE

Selecteer de bestanden, die je wilt inpakken.
Stap 1.
Rechtsklik op de gekozen bestanden en/of hoofdmap en kies voor "7-Zip".
Stap 2.
Kies voor de optie uit het keuzemenu: "Toevoegen aan archief". Alle bestanden en onderliggende mappenstructuur zullen in één nieuw bestand samengebald worden.
Stap 3.
Voer in het dialoogvenster aan de rechteronderkant bij "Codering" een sterk wachtwoord in en herhaal dit wachtwoord. Standaard gebruik je hierbij AES256 versleuteling, controleer dit.

2. Uitpakken van bestanden en/of mappen uit het 'moeder'bestand.

Uitpakken gaat op een vergelijkbare wijze.
Stap 1.
Rechtsklik op het samengebalde bestand in de door jou gekozen locatie en kies voor "7-Zip".
Stap 2.
Kies daarna uit het keuzemenu: "Pak uit naar map "xxx"". Alle bestanden en onderliggende mappenstructuur worden in deze map uitgepakt.
Stap 3.
Het programma zal je vragen om het wachtwoord in te voeren, dit is eenmalig noodzakelijk.

CS R02 - Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS

Doelgroep
Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van de Opdrachtgever.

Doel
Deze richtlijn heeft als doel om cybersecurity risico's te mitigeren ingeval medewerkers van de Opdrachtnemer voor het verrichten van beheer- en onderhoudswerkzaamheden apparatuur zoals draagbare media (USB-stick, externe disk, laptop, tablet, CD's, DVD's) moeten koppelen aan de ICT, PLC's Servers, Routers, Switches, etc. binnen de ICT en IA omgevingen van Rijkswaterstaat.

Randvoorwaarden
Medewerkers
Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van Rijkswaterstaat hebben een bewustwordingstraining voor cybersecurity gevolgd, bij voorkeur toegespitst op SCADA systemen.

Apparatuur
Actieve apparaten
Onder actieve apparaten wordt verstaan: laptops, tablets.
Voor deze apparatuur gelden de volgende maatregelen:
- hardening;
- malwarescanning;
- (interne) firewall;
- encryptie van de interne harddisk(s).

NOOT: *Smartphones mogen niet worden ingezet voor beheer en onderhoudswerkzaamheden, aangezien zulke apparatuur niet kan voldoen aan de door Rijkswaterstaat gestelde veiligheidseisen.*

Passieve apparaten
Onder passieve apparaten worden gegevensdragers en opslagmedia verstaan: diskettes, CD-ROM's, DVD's, USB-sticks en externe disks.
Voor deze apparaten gelden de volgende maatregelen:
- gebruik uitsluitend voor beheer en onderhoud op ICT en IA systemen van Rijkswaterstaat
- encryptie van USB-sticks en externe disks
- malwarescanning voorafgaand aan gebruik op ICT en IA systemen

Instructies
Voor het beveiligingsbewust omgaan en het veilig koppelen van apparaten aan de ICT en IA systemen van Opdrachtgever gelden de volgende instructies.

<u>*Actieve apparaten*</u>

Initiële maatregelen
1. Zorg dat het apparaat 'gehardend' is. Zie bijlage A.
2. Zet encryptie van de disk in het apparaat aan. Zie bijlage A.
3. Beveilig de toegang tot het apparaat met een sterk wachtwoord. Zie bijlage A.
4. Installeer een malwarescanner.
5. Zet de interne firewall aan.

Maatregelen tijdens gebruik

Vertrouwelijkheid: RWS INFORMATIE

1. Gebruik het apparaat uitsluitend voor beheer en onderhoud van IA systemen van Rijkswaterstaat.
2. Zet 3G, 4G, WiFi en Bluetooth uit tijdens het gebruik op de objecten van RWS. (koppelingen tussen IA en andere netwerken zijn niet toegestaan)
3. Zorg vooraf voor de meest recente updates en patches van het OS van het apparaat.
4. Zorg vooraf voor de meest recente updates van de malwarescanner.
5. Download geen updates, ook niet voor ICT of IA systemen van Rijkswaterstaat, als het apparaat aan ICT of IA systemen van Rijkswaterstaat is gekoppeld. Updates en patches voor ICT of IA systemen dienen gedownload te zijn voordat de draagbare media word gekoppeld aan het ICT of IA systeem.
6. Check of downloads van ICT of IA-software uit een betrouwbare bron komen door te controleren op de meegeleverde hashcode.
7. Download ICT of IA-software uitsluitend via een beveiligde (https) verbinding.
8. Check downloads (van IA-software) op malware voordat de downloads ingezet worden binnen de ICT of IA omgeving.

Passieve apparaten (opslagmedia)

1. Gebruik opslagmedia voor ICT of IA systemen bij Rijkswaterstaat niet voor andere doeleinden.
2. Zorg dat de gegevens op USB-sticks en externe harddisks encrypt zijn.
3. Scan diskettes, CD-ROM’s, DVD’s, USB-sticks en externe disks elke keer voordat deze gebruikt gaan worden op malware.
4. Vervang een opslagmedium waarop malware is ontdekt voor een nieuw opslagmedium.

Bijlage A bij CS R02

Hardening
Hardening is het verwijderen van overbodige functionaliteit van een apparaat. Vooral het 'hardenen' van een Operating System (Microsoft Windows, Linux, iOS, Android) zorgt er voor dat het apparaat minder kwetsbaar is voor besmetting met malware.
Op het internet zijn standaard hardeningsprofielen beschikbaar voor de meeste platformen zie bijv. de 'Security Benchmarks' van CIS: http://www.cisecurity.org/
Het uitzetten van Active-X controls en Adobe Flash is een vorm van hardening waarmee de kans op malware besmetting verkleind wordt.

Voor Microsoft platforms kan de Microsoft Baseline Security Analyzer (MBSA) een hulpmiddel zijn om ontbrekende security updates of foutieve instellingen van security parameters te kunnen checken. Dit kan en mag alleen ingezet worden wanneer met zekerheid gesteld kan worden dat de inzet hiervan geen risico vormt voor de continuïteit van het systeem.

Encryptie
Voor encryptie dient AES256 versleuteling te worden toegepast.

Sterk wachtwoord
Een sterk wachtwoord voor IA systemen is minimaal 15 karakters lang en bestaat uit een combinatie van Hoofdletters, kleine letters, cijfers en symbolen (bijvoorbeeld !, # of &) en mag geen volledig woord of naam zijn.

Malware
Schadelijke software zoals virussen, trojans, enzovoort die (ICT of IA-)systemen kunnen besmetten met mogelijk storingen of ongewenste effecten in de bediening als gevolg.

Q&A

Q: Waarom opslagmedium waarop malware is ontdekt vervangen voor een nieuw opslagmedium?
A: Malware wordt steeds intelligenter en is in staat zich zodanig op (de BIOS van) een apparaat te nestelen dat deze er niet meer af te krijgen is.

Vertrouwelijkheid: RWS INFORMATIE

CS R03 - Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging

Doelgroep
Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van opdrachtgever.

Doel
Deze richtlijn heeft als doel om inzicht te bieden en richting te geven aan de acties die medewerkers van de Opdrachtnemer moeten nemen als er sprake is van een hack of een malwarebesmetting . Tevens zijn richtlijnen opgenomen voor de handelwijze van de Opdrachtnemer als door Rijkswaterstaat is aangegeven dat er sprake is van verhoogde dreiging.

Scenario's
Deze richtlijn betreft de volgende scenario's:
1. Hack: één of meer IA systemen zijn of worden gehacked
2. Malware besmetting: één of meer IA systemen zijn besmet met malware
3. Verhoogde dreiging: er is een verhoogde dreiging op een hackaanval op IA systemen van Rijkswaterstaat.

Hack
Als het object in beweging is gebracht, zonder dat de bedienaar hier bewust opdracht toe heeft gegeven via het ICS/SCADA systeem, dan is er mogelijk sprake van een cyberaanval op het object. De Opdrachtnemer wordt via een storingsmelding van de bedienaar opgeroepen om ter plaatse te komen.
De monteur van de Opdrachtnemer neemt de volgende stappen:
1. Vraag aan de bedienaar wat er precies aan de hand is
   (indien het object onverwachte en 'onbeheersbare' acties blijft vertonen dan zal de bedienaar het object veiligstellen);
2. Controleer mogelijke storingen aan het IA-systeem op de gebruikelijke manier;
3. Onderzoek, indien aanwezig, de logs van het betreffende IA systeem dat het object bedient op onregelmatigheden;
4. Stel, zo mogelijk, vast dat het niet om een technische storing gaat;
5. Rapporteer via het storingsproces de bevindingen terug naar de opdrachtgever;
6. Afhankelijk van de door de monteur gerapporteerde bevindingen kunnen nadere instructies vanuit opdrachtgever volgen die door de monteur opgevolgd moeten worden om er zeker van te zijn dat het om een hack(poging) gaat;
7. Als er daadwerkelijk sprake is van een hack(poging) informeer dan de betrokkenen van de regio (bedienaars, Officier van Dienst, etc.).

Malware besmetting
Als (bijvoorbeeld tijdens een reguliere onderhoudsbeurt) er een (vermoeden van een) malware besmetting op het object is, dient door de monteur van de Opdrachtnemer de volgende acties te worden genomen:
1. Meld een mogelijke malware besmetting op de reguliere manier als het melden van storingen onder vermelding van mogelijk risico op malwarebesmetting en geef alle bevindingen door;
2. Het oplosteam van Opdrachtgever zal contact zoeken met de monteur voor afstemming van de uit te voeren acties;
3. Wijzig niets aan het systeem als dat voor een veilige werking van het object niet strikt noodzakelijk is;
4. Maak, indien de opdrachtgever daar om vraagt conform zijn instructies, een volledige image van de (systeem)software van het betreffende IA systeem / -onderdeel;
5. Stel deze image van de (systeem)software ter beschikking aan de opdrachtgever voor nader onderzoek;

6. Wees alert op onverwachte bewegingen / storingen van het object en informeer de bedienaar om hier ook alert op te zijn;
7. Indien er (eventueel na onderzoek door de opdrachtgever) sprake blijkt te zijn van malware besmetting, controleer dan (of laat dit door de opdrachtgever doen) of de backup ook is besmet;
8. Indien er sprake is van een malwarebesmetting en de backup blijkt niet geinfecteerd, zet dan de backup terug op het systeem;
9. Als ook de backup besmet is, zorg er dan voor dat de besmette image 'geschoond' wordt en zet de geschoonde versie terug. De opdrachtgever kan hier ondersteuning bij bieden;
10. Let op dat de juiste parameters zijn ingesteld;
11. Meld de storing op de reguliere manier af.

Verhoogde Cyberdreiging
Er is sprake van verhoogde cyberdreiging als blijkt dat er een mogelijke aanval op objecten van Rijkswaterstaat op handen is. Er hoeft daarbij nog geen sprake te zijn van een daadwerkelijke hackaanval. Soms worden deze aanvallen aangekondigd door de groepering die deze aanval gaat uitvoeren soms kan deze informatie ook uit andere bronnen zijn verkregen waarbij het minder duidelijk is op welk moment de aanval kan plaatsvinden. Alertheid is daarom geboden.
Een aantal objecten van Rijkswaterstaat zijn aangesloten op het proces en Alerteringssysteem Terrorismebestrijding (ATb) van het ministerie van Veiligheid en Justitie.

Indien er sprake is van een verhoogde cyberdreiging dan meldt het Departementaal Coördinatiecentrum Crisisbeheersing (DCC) van het ministerie van Infrastructuur en Milieu dit aan het lijnmanagement van Rijkswaterstaat als de dreiging op een specifiek object is gericht.

De Opdrachtnemer wordt vervolgens via het storingsmeldingsproces op de hoogte gebracht van de verhoogde dreiging.

De Opdrachtnemer neemt de volgende acties:

1. De Opdrachtnemer neemt naar aanleiding van de storingsmelding contact op met de door de opdrachtgever aangegeven contractpersoon voor afstemming van uit te voeren acties en het tijdstip waarop deze acties nodig zijn;
2. Indien er sprake is van een acute dreiging dan zorgt de Opdrachtnemer er voor dat, afhankelijk van het verzorgingsgebied van de Opdrachtnemer, er voldoende monteurs standby zijn om de objecten in dat verzorgingsgebied te 'servicen';
3. Indien er daadwerkelijk hacks plaatsvinden dan gelden de stappen onder **Hack.**

Vertrouwelijkheid: RWS INFORMATIE

CS R04 - Richtlijn continuiteitsplan

Het continuïteitsplan beschrijft per object de acties die door de Opdrachtnemer moeten worden uitgevoerd om voorbereid te zijn op het herstel na storingen van systemen. In geval van omvangrijke storingen is het functioneren van de kritieke ICT en IA systemen geborgd en spoedig herstel na storingen wordt hiermee mogelijk.

De scope van het continuïteitsplan omvat alle kritieke ICT en IA systemen en de daarvoor benodigde energie voorzieningen die noodzakelijk zijn voor de functioneren en veilige werking van het object.

Per object dient een continuïteitsplan te worden opgesteld dat ten minste het volgende omvat:

1. Risicoanalyse en afweging
   Een risicoanalyse en risicoafweging gebaseerd op de functionele kaders die door de opdrachtgever zijn meegegeven en de ontwerpkeuzes die door de Opdrachtnemer zijn gemaakt, om de kritieke ICT en IA systemen, applicaties services en de benodigde back-up voorzieningen voor software en de daarvoor benodigde energievoorzieningen in beeld te brengen.
2. Overzicht van systemen, applicaties en services en back-up voorzieningen
   Een overzicht van alle kritieke ICT en IA systemen, applicaties en services die hersteld of opgestart moeten worden in het geval van uitval van de primaire energie voorzieningen (zoals elektriciteit) of een omvangrijke storing in de ICT of IA systemen.
3. Overzicht van alle noodzakelijke systeemdocumentatie
   Een overzicht van actuele documentatie die benodigd is om de ICT en IA systemen, applicaties en services te herstellen na een omvangrijke storing. Tot de documentatie behoren ook de benodigde accounts en wachtwoorden voor de onderkende systemen alsmede de documentatie van de nood voorzieningen voor energie en de back-up voorzieningen voor software. De documentatie dient zowel digitaal als in hardcopy op twee fysiek gescheiden locaties bewaard te worden.
4. Organisatie en borging continuïteitsbeheer
   Een beschrijving van de wijze waarop het beheer en onderhoud van het continuïteitsplan is belegd in de (project)organisatie van de Opdrachtnemer. Tevens dient er een overzicht te zijn van rolhouders, hun bereikbaarheid en vervangers inclusief hun verantwoordelijkheden en bevoegdheden.
5. Continuïteitsplan
   Een beschrijving van situaties waarin het continuïteitsplan wordt geactiveerd door een geautoriseerde functionaris en de wijze van afschaling.
6. Periodieke beproeving en onderhoud van het continuïteitsplan
   Een beschrijving op welke wijze het continuïteitsplan minimaal jaarlijks wordt beproefd, alsmede een beschrijving van de wijze waarop het continuïteitsplan na iedere activaring wordt geëvalueerd en geactualiseerd. Hierbij dient nadrukkelijk aandacht te worden besteed aan de werking van back-up en recovery proces voor software alsmede aan de (nood) energievoorzieningen en gerelateerde voorraden hiervan.

CS R05 - Richtlijn camera’s en omgang met camerabeelden van de verkeersregistratiesystemen

Binnen de verkeersregistratiesystemen van Rijkswaterstaat worden tegenwoordig veel videocamera's ingezet. Het betreft bijvoorbeeld camera's bij tunnels, wisselstroken, spitsstroken, sluizen en bruggen. Reden voor het gebruik van videocamera's kan zijn het bevorderen van veiligheid van het verkeer, maar ook het op afstand regelen van waterstaatswerken, zoals bruggen. Dergelijke videocamera's zijn meestal gekoppeld aan systemen waarmee beelden kunnen worden vastgelegd. Beelden kunnen persoonsgegevens bevatten. Een voorbeeld van een persoonsgegeven is een videobeeld indien daarop een persoon zichtbaar is of gegevens staan die herleidbaar zijn tot een natuurlijk persoon. Persoonsgegevens moeten conform de Wet Bescherming Persoonsgegevens (Wbp) beveiligd worden.

Doelgroep
Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden verrichten aan camera’s en systemen die camerabeelden opslaan, verwerkt of distribueert.

Doel
Deze richtlijn heeft als doel om medewerkers van de Opdrachtnemer bewust te maken van de privacy aspecten wanneer ze in contact komen met camera’s en systemen waarin camerabeelden worden opgeslagen, verwerkt of gedistribueerd en de hieronder beschreven instructies in acht nemen bij het verrichten van hun werkzaamheden.

Randvoorwaarden
Medewerkers
Medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van Rijkswaterstaat hebben een bewustwordingstraining voor cybersecurity gevolgd waarbinnen ook aandacht is besteed aan het vertrouwelijk omgaan met persoonsgegevens. Voor deze medewerkers geldt verder dat zij strikte geheimhouding in acht nemen en over een Verklaring Omtrent het Gedrag (VOG) beschikken zoals contractueel overeengekomen.

Instructies
Voor het beveiligingsbewust omgaan met camera’s en systemen waarin camerabeelden worden opgeslagen gelden de volgende instructies:

1. Alleen geautoriseerde medewerkers van de Opdrachtnemer mogen beheer- en onderhoudswerkzaamheden uitvoeren aan camera’s en systemen die camerabeelden opslaan;
2. De eventueel benodigde en verkregen accounts en wachtwoorden zijn strikt voor persoonlijk gebruik en mogen niet met anderen worden gedeeld. Hieronder vallen de accounts en wachtwoorden en toegangsmiddelen tot ruimten en de toegang tot de systemen binnen de ruimten;
3. Zonder uitdrukkelijke toestemming van de opdrachtgever worden camerabeelden niet vernietigd, verwijderd of verstrekt aan derden of gebruikt voor persoonlijke of bedrijfsdoeleinden;
4. Indien bestanden met camerabeelden tijdelijk opgeslagen moeten worden of een kopie gemaakt moet worden voor onderzoeksdoeleinden is zorgvuldige omgang vereist. Er dient hierbij altijd een beveiligingsmaatregel actief te zijn zodat alleen een geautoriseerde medewerker toegang kan verkrijgen tot het bestand met beelden met in achtneming van de vigerende wachtwoord policy. Voorbeeld is dat bestanden op een beveiligde usb-stick of laptop met encryptie van de harde schijf worden opgeslagen en ontsluiting via een wachtwoord plaatsvindt. Standaard dient hierbij AES-256 versleuteling gebruikt te worden;

Vertrouwelijkheid: RWS INFORMATIE

5. Na afronding van de werkzaamheden dient controle plaats te vinden dat er geen onnodige kopieën van bestanden met camerabeelden op eigen apparatuur of media en/of back-ups achterblijft;
6. Indien onregelmatigheden worden geconstateerd rondom de inzet, werking en opslag van camerabeelden dient dit direct als beveiligingsincident bij de opdrachtgever gemeld te worden.

CS R06 - Richtlijn registratie CI items in een configuration management database

Een actuele configuration management database maakt het de opdrachtgever mogelijk om proactief cybersecurity kwetsbaarheidsanalyses uit te kunnen voeren en de beheerders te adviseren over maatregelen alsmede het kunnen analyseren van security incidenten of storingen. Derhalve moet de opdrachtgever vanuit een informatievoorzieningsketen benadering kunnen leunen op de kwaliteit van de afzonderlijke configuration management databases die door de afzonderlijke opdrachtnemers worden opgezet en bijgehouden.

De Opdrachtnemer dient in het kader van cybersecurity dan ook ten minste de volgende gegevens van alle configuration items (CI) in de configuratie management database (CMDB) te registreren en actueel te houden:

		Waarde	Definitie	Schrijfwijze
1	**Type en merk ICT en/of ICS/SCADA apparatuur**			
	Type		Type ICT en/of ICS/SCADA apparatuur	
	Merk		Merk ICT en/of ICS/SCADA apparatuur	
	Soort ICT/ICS/SCADA		Soort ICT/ICS/SCADA	LOV: ICT; ICS; SCADA
	Ordernummer vendor			
2	**Producent en Leverancier**			
	Producent		Overkoepelende naam, waaronder de `Producent` zijn applicaties verkoopt.	Naam van de handelsnaam van de applicatie op de box, zonder juridische bedrijfsvorm of andere toevoegingen.
	Leverancier		Leverancier	
3	**Versienummer van ICT en/of ICS/SCADA apparatuur**			
	Versie		Versie ICT en/of ICS/SCADA apparatuur	
4	**Formaat van de apparatuur**			
	Formaat		Lengte, Breedte en Hoogte	
5	**Type object en locatiegegevens**			
	Type object		Type object	LOV: Brug; Sluis; etc.
	Locatiegegevens		Fysiek adres	Naam, Straat, Huisnummer, Postcode, Plaats
6	**Ingezette software en hardware componenten inclusief hun samenhang en configuratie**			
	Software		Naam van de applicatie, zoals uitgegeven door de `Producent`. Indien er zowel een `Volledige naam` als een afkorting bestaat, dient hier de afkorting te worden ingevuld.	Naam van de applicatie op de box. Indien er zowel een `Volledige naam`

Vertrouwelijkheid: RWS INFORMATIE

		Waarde	Definitie	Schrijfwijze
				als een afkorting bestaat, dient hier de afkorting te worden ingevuld.
	Hardware		Een specifieke variatie of verdere ontwikkeling van een origineel stuk software.	Zonder voorloop-V, nummers gescheiden door punten.
	Configuratie		Relatie "Bestaat uit" en tegenrelatie "Is onderdeel van"	
7	**Informatie over de back-up voorziening**			
	Back-up voorziening			
8	**Datum laatste back-up en locatie van de back-up**			
	Datum laatste back-up		Datum laatste back-up	ISO 8601 formaat: jjjj-mm-dd
	Locatie van de back-up		Fysiek adres	Naam, Straat, Huisnummer, Postcode, Plaats
9	**OS (Operation System), versie OS en Firmware**			
	OS (Operation System)		Naam van de applicatie, zoals uitgegeven door de `Producent`. Indien er zowel een `Volledige naam` als een afkorting bestaat, dient hier de afkorting te worden ingevuld.	Naam van de applicatie op de box. Indien er zowel een `Volledige naam` als een afkorting bestaat, dient hier de afkorting te worden ingevuld.
	Versie OS			
	Versie Firmware		Versie Firmware	
10	**Ingezette netwerk en applicatieprotocollen**			
	Applicatie Protocollen			LOV: SOAP, JSON,
11	**licentie informatie en verloopdatum licentie**			
	Verloopdatum licentie		De datum, waarop het contract zijn rechtsgeldigheid verliest.	ISO 8601 formaat: jjjj-mm-dd
12	**Escrow documentatie**			
	Escrow documentatie			
13	**Antimalware geïnstalleerd ja/nee**			
	Antimaleware geïnstalleerd		Antimaleware geïnstalleerd	LOV: Ja; Nee
14	**Welke antimalware applicatie en versie**			

		Waarde	Definitie	Schrijfwijze
	Applicatie Naam		Relatie Applicatie gebruikt Applicatie (Antimaleware)	
	Applicatie Versie		Relatie Applicatie gebruikt Applicatie (Antimaleware)	
15	**Netwerkoverzichten fysieke en logisch en IP-plan**			
	Fysiek Netwerkoverzicht		Fysiek Netwerkoverzicht	
	Logisch netwerkoverzicht		Logisch netwerkoverzicht	
	IP-plan		IP-plan: • VICnet switch poort • Hostname RWS • Onderdeelcodering Project • Systeem Functie (bv handheld) • Source IP adres • Netwerk (bv 10.117.160.0) • Subnetmask (bv 255.255.255.224) • Default Gateway (bv 10.117.160.1) • Source VLAN nummer (bv 550) • Source type (bv INTERCOM) • Ring (bv GELDW R6) • Source VPN (bv VPN-HWN :PRO-BOA) • VLAN overzicht (bv 550, DATA, VPN-VICNET:VICNET)	
16	**IP- en MAC-adres, DNS en hostnaam**			
	IP-adres		IP-adres	
	MAC-adres		Mac-adres	
	DNS		Domain Name Server Relatie "Gebruikt Server"	
	Hostnaam		Hostnaam	
17	**Documentatie patch procedure**			
	Patch documentatie			
18	**Datum laatste patch en versie**			
	Datum		Patch documentatie datum	ISO 8601 formaat: jjjj-mm-dd
	Versie		Patch versie	
19	**Vervangingsinstructie en/of –procedure voor apparaat**			
	Vervangingsinstructie en/of –procedure voor apparaat;			
20	**Identificatie en verwijzing naar vindplaats gebruikers-, beheer- en onderhoudsdocumentatie**			
	Identificatie			
	Verwijzing naar vindplaats gebruikers-, beheer- en onderhoudsdocumentatie		Verwijzing naar vindplaats gebruikers-, beheer- en onderhoudsdocumentatie	
21	**Datum laatst gewijzigd en door wie**			
	Updated		Laatst gewijzigd datum	ISO 8601 for-

		Waarde	Definitie	Schrijfwijze
				maat: jjjj-mm-dd
	Persoon		Laatst gewijzigd door	Achternaam, Voornaam tussenvoegsel

Deze gegevens dienen conform de contractueel overeengekomen informatieleveringen in excelformaat aangeleverd te worden.

Definitie Configuration Item (CI): een component deel uitmakende van of direct gerelateerd aan de ICT of IA zoals documentatie.

Deel 3: Template Plan Cybersecurity

Template

Plan Cybersecurity <20XX>

voor

<<<<object, installatie, dienst(verlening)>>>>

Opdrachtnemer/Uitvoerder	
Naam	
Functie	
Datum	
Status	
Classificatie	Vertrouwelijk (*na invulling door ON*)
Paraaf	

Vertrouwelijkheid: RWS INFORMATIE

Colofon

1. Inleiding

Uitgegeven door	RWS/CIV/IRN/Security Centre
Informatie	
Opmaak	
Datum	06 oktober 2015
Versienummer	1.0

1.1 Doel

De doelstelling van dit document is om een template voor de Opdrachtnemer beschikbaar te stellen waarmee de risico's met betrekking tot cybersecurity zodanig kunnen worden beheerst dat de betrouwbaarheid (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) van de installatie, het object of de dienst(verlening) gedurende de looptijd van de Overeenkomst wordt gewaarborgd.

De Opdrachtnemer is vrij in het gebruik van deze template en kan ook een eigen template gebruiken, mits minimaal de informatie-elementen uit dit document zijn opgenomen.

1.2 Scope

Onder de scope van het Plan Cybersecurity vallen:
de Opdrachtnemer beschrijft hier wat wel en niet onder de areaalscope van dit Plan Cybersecurity valt.

2 Risico's

2.1 Risico's

De beheersing van de toegang, of het nu fysiek of digitale vorm is, vormt letterlijk en figuurlijk het sleutelbegrip voor het terugdringen van de cybersecurity risico's voor de infrastructuur van Rijkswaterstaat.

De mitigatie van de volgende risico's zijn vanuit de Opdrachtgever geprioriteerd:

1. Niet-geautoriseerden hebben fysieke toegang tot bedien- en technische ruimten;
2. Niet-geautoriseerden hebben logisch toegang tot de ICT en ICS/SCADA-systemen van RWS;
3. Informatie over zwakke plekken in de beveiliging en beveiligingsincidenten ontbreekt alsmede een handelingsperspectief;
4. Niet-geautoriseerden hebben (via Internet of draadloze toepassingen) toegang tot het RWS datanetwerk;
5. Risico's geïntroduceerd door (zelfstandige) hulppersonen. Deze zijn zich niet bewust van onveilige situaties, beschikken niet over de juiste opleiding en training, hebben geen geheimhoudingsverklaring getekend of beschikken niet over een recente verklaring omtrent het gedrag;
6. Functionele wijzingen brengen onvoorziene veiligheid- en beveiligingseffecten met zich mee en kunnen zelfs de functionele werking van ICT en IA-systemen deels of volledig doen uitvallen;
7. De handhaving en de effectiviteit van de Cybersecuritymaatregelen is niet gewaarborgd alsmede de structurele borging bij onderaannemers;
8. Bij systeemstoringen of functionele wijzigingen is er geen terugvaloptie (geen back-up en recovery proces).

Vertrouwelijkheid: RWS INFORMATIE

3 Cybersecurity beheersmaatregelen

De Opdrachtnemer werkt minimaal de volgende items uit.

3.1 Comply or explain
De Opdrachtnemer motiveert in deze paragraaf welke cybersecurity eisen uit de Overeenkomst voor betreffende object, installatie of dienst(verlening) niet of afwijkend worden ingevuld in relatie tot de scope van het Plan Cybersecurity, zoals beschreven in paragraaf 1.2 voor de betreffende installatie, object of dienst(verlening).

3.2 Risico's
De Opdrachtnemer beschrijft hier de risico's die door de Opdrachtgever zijn aangereikt en die naar voren komen uit de periodiek door de Opdrachtnemer uit te voeren risicoanalyse en risicoafweging zoals vereist in de Overeenkomst of de Cybersecurity Implementatierichtlijn Objecten - RWS. Indien de door de Opdrachtgever aangegeven risico's niet van toepassing zijn voor de betreffende installatie, object of dienst(verlening), dan dient dit gemotiveerd te worden bij paragraaf 3.1 waar de 'comply or explain' regel geldt.

3.3 Beheersmaatregelen
De Opdrachtnemer beschrijft de voor dit object getroffen cybersecurity beheersmaatregelen inclusief de jaarlijks evaluatie en indien nodig bijstelling.

3.3.1 Belegging verantwoordelijkheden
De Opdrachtnemer beschrijft hoe de verantwoordelijkheid voor cybersecurity is belegd binnen zijn organisatie, het eerste aanspreekpunt voor cybersecurity aangelegenheden voor de Opdrachtgever en zijn of haar vervanging bij afwezigheid van het eerste aanspreekpunt

3.3.2 Borging Cybersecurity
De Opdrachtnemer beschrijft hoe de cybersecurity beheersmaatregelen in zijn managementsysteem zijn geborgd.

3.3.3 Onderaannemers
De Opdrachtnemer beschrijft op welke wijze de cybersecurity eisen geborgd zijn bij gebruik van onderaannemers die in aanraking komen met de getroffen cybersecurity beheersmaatregelen of het beheer en onderhoud van de cybersecurity maatregelen verzorgen.

3.3.4 Beheer bedrijfsmiddelen, CMDB
De Opdrachtnemer beschrijft conform richtlijn CS R06 op welke wijze de configuration items van alle ICT en IA (waaronder ICS/SCADA-systemen) worden geregistreerd in een CMDB en hoe de actualiteit van deze wordt gewaarborgd. Ook dient beschreven te worden op welke wijze deze informatie aan de Opdrachtgever beschikbaar wordt gesteld.

3.3.5 Aanvaardbaar gebruik toegangsmiddelen
De Opdrachtnemer beschrijft op welke wijze de Opdrachtnemer een aanvaardbaar gebruik van door de Opdrachtgever eventueel beschikbaar gestelde toegangsmiddelen (pasjes, tokens, e.d.) bewerkstelligt en een sluitende administratie bijhoudt aan de kant van de Opdrachtnemer.

3.3.6 Classificatie en beveiliging informatie
De Opdrachtnemer beschrijft conform richtlijn CS R01 omgaan met vertrouwelijke informatie en documenten op welke wijze de beveiliging wordt bewerkstelligd van de door de Opdrachtgever aangegeven vertrouwelijke documenten, zoals ontwerp, constructietekeningen en datanetwerkschema's.

3.3.7 Bewustwording, scholing en VOG
De Opdrachtnemer beschrijft op welke wijze het personeel bewust wordt gemaakt van de cybersecurity risico's, aantoonbaar over de juiste opleiding, training en vaardigheden beschikt en geheimhouding in acht neemt.

3.3.8 Fysieke toegangsbeveiliging
De Opdrachtnemer beschrijft op welke wijze de fysieke toegangsbeveiliging tot het object, de IA-gerelateerde en technische ruimten wordt beheerst of op controleerbare manier aansluit op het fysieke toegangsbeheerproces van de Opdrachtgever.

3.3.9 Logische toegangsbeveiliging tot ICT en IA-systemen
De Opdrachtnemer beschrijft op welke wijze de logische toegangsbeveiliging tot de ICT en IA-systemen wordt beheerst of op controleerbare manier aansluit op het logische toegangsproces van de Opdrachtgever.

3.3.10 Wachtwoordrichtlijn
De Opdrachtnemer beschrijft op welke wijze invulling wordt gegeven aan de door de Opdrachtgever beschikbaar gestelde wachtwoordrichtlijn. De Opdrachtnemer geeft gemotiveerd aan of er afwijkingen bestaan.

3.3.11 Back-up en recovery proces
De Opdrachtnemer test jaarlijks voor zover back-up en recovery voorzieningen bestaan het back- up recovery proces.

3.3.12 Beveiliging documentatie
De Opdrachtnemer beschrijft op welke wijze de beheer en technische documentatie in zijn organisatie beschermd wordt tegen verlies en ongeautoriseerde kennisname of wijziging.

3.3.13 Wijzigingsproces
De Opdrachtnemer beschrijft hier het wijzigingsproces die gevolgd wordt voor het doorvoeren van (functionele) wijzigingen aan ICT en IA conform de eisen uit de overeenkomst en de Cybersecurity Implementatierichtlijn Objecten - RWS.

3.3.14 Beveiliging tegen malware, hardening en patching
De Opdrachtnemer beschrijft, voor zover voorzieningen en inrichtingen aanwezig zijn, voor hardening, malware en patching en op welke wijze het onderhoud hierop vormt krijgt.

3.3.15 Patch proces en kritieke Patches
De Opdrachtnemer beschrijft op welke wijze het patchproces wordt vormgegeven zowel qua proces als de hiervoor gebruikte voorzieningen en hoe de risicoafweging plaatsvindt inclusief de formulering van het advies aan de Opdrachtgever conform de eisen uit de Cybersecurity Implementatierichtlijn Objecten - RWS.

3.3.16 Koppeling van apparatuur
De Opdrachtnemer beschrijft conform richtlijn CS R02 veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS op welke wijze de bescherming tegen malware (waaronder virussen) wordt vormgegeven qua proces en voorzieningen bij koppeling van mobiele apparatuur of removable media aan de ICT en IA van de Opdrachtgever door de Opdrachtnemer of zijn (zelfstandige) hulppersonen.

3.3.17 Logging en monitoring
De Opdrachtnemer beschrijft, indien logvoorzieningen aanwezig zijn op de bestaande ICT en IA, op welke wijze wordt omgegaan met de logbestanden en hoe op verzoek van de Opdrachtgever deze aan de Opdrachtgever ter beschikking worden gesteld.

Vertrouwelijkheid: RWS INFORMATIE

3.3.18 Datanetwerkkoppelingen
De Opdrachtnemer beschrijft hoe het bijwerken van netwerkschema's plaatsvindt naar aanleiding van wijzigingen op datanetwerkkoppelingen.

3.3.19 Remote Access
De Opdrachtnemer beschrijft of er sprake is van remote acces voor beheer en onderhoud van ICT en IA en hoe geborgd is dat dit conform de eisen hieraan verloopt.

3.3.20 Gebruik veilige communicatieprotocollen
De Opdrachtnemer beschrijft indien configuratie van de ICT en IA (waaronder ICS/SCADA) buiten de door de Opdrachtgever beschikbaar gestelde dienst op afstand plaatsvindt welke communicatieprotocollen hiervoor worden ingezet en of deze veilig zijn.

3.3.21 Webapplicaties
De Opdrachtnemer beschrijft indien (web)applicaties worden ingezet voor beheer op afstand hoe de beveiliging is vormgegeven.

3.3.22 Continuïteit en herstel dienstverlening
De Opdrachtnemer beschrijft voor zover door Opdrachtgever beschikbaar gesteld op welke wijze hij de continuiteitsplannen onderhoud.

3.3.23 Testen continuïteitsplannen
De Opdrachtnemer beschrijft voor zover door de Opdrachtgever beschikbaar gesteld op welke wijze de continuïteitsplannen periodiek worden getest en geactualiseerd.

3.3.24 Beveiliging Spionage
De Opdrachtnemer beschrijft welke maatregelen er in zijn organisatie voor de beveiliging tegen spionage zijn getroffen.

3.3.25 Beveiliging van de Informatievoorziening
De Opdrachtnemer beschrijft op welke wijze geclassificeerde informatie en documenten, zoals aangegeven door de Opdrachtgever, zijn beveiligd tegen verlies, ongeautoriseerde kennisname of wijziging bij verwerking in de kantoor- en netwerkomgeving van Opdrachtnemer.

3.3.26 Cybersecurity inbreuken en verhoogde dreiging
De Opdrachtnemer beschrijft conform richtlijn CS R03 handelwijze bij een hack, malwarebesmetting en verhoogde dreiging welk proces er is ingericht en gevolgd wordt indien de Opdrachtgever melding maakt van Cybersecurity inbreuken (incident response proces) en bij verhoogde dreiging.

3.3.27 Security gerelateerde wijzigingen
De Opdrachtnemer beschrijft hier op welke wijze security gerelateerde wijzigingen worden beoordeeld op mogelijke impact en risico's alvorens de wijziging wordt doorgevoerd.

4 Jaarlijkse toestandsrapportage cybersecurity

De opdrachtnemer werkt minimaal de volgende items uit.

4.1 Bevindingen
De Opdrachtnemer beschrijft hier de maatregelen die hij neemt o.b.v. de bevindingen die voortvloeien uit de jaarlijkse cybersecurity audit.

4.2 Analyse cybersecurity incidenten
De Opdrachtnemer beschrijft hier de maatregelen die hij neemt o.b.v. de resultaten van de analyse van alle cybersecurity incidenten die zich de afgelopen periode (jaar) hebben voorgedaan en gemeld zijn aan de Opdrachtgever in de tussentijdse toestandsrapportages.

4.3 Testresultaten back-up en recovery proces
De Opdrachtnemer beschrijft hier de maatregelen die hij neemt o.b.v. de resultaten van de jaarlijkse beproevingen van het back-up voorzieningen en recovery proces voor zover deze bestaan in het Areaal.

4.4 Testresultaten continuiteitsplannen en -voorzieningen
De Opdrachtnemer beschrijft hier de maatregelen die hij neemt o.b.v. de resultaten van de jaarlijkse beproevingen van de continuiteitsplannen en -voorzieningen voor zover deze bestaan in het Areaal.

4.5 Risicoanalyse en risicoafweging
De Opdrachtnemer beschrijft hier de maatregelen die hij neemt o.b.v. de resultaten van de jaarlijks uit te voeren risicoanalyse en risicoafweging waarbij ook de resultaten van de paragrafen 4.1 t/m 4.4 ook in beschouwing worden genomen.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage W Invulinstructie format LV BRO

Attribuut	Invulinstructie
Bronhouder	**27364178** *(ALTIJD)* *Toelichting: het KvK nummer van Rijkswaterstaat ter identificatie als bestuursorgaan*
Object-ID	<Vul WBS-element in> *Toelichting: het 'WBS-element niveau 2' uit SAP invullen ten behoeve van de Opdrachtnemer. Met behulp van dit nummer kan RWS ook op lange termijn de interne opdrachtgever en opdrachtnemer achterhalen; tevens is het mogelijk om alle onderliggende elementen te vinden. Een WBS-element is altijd als volgt opgebouwd: een letter, een punt, acht cijfers, een punt, vier cijfers. Dus bijvoorbeeld P.00000183.0002.* *Niet bekend met het nummer? Vraag het de betrokken adviseur bedrijfsvoering.*
Data-leverancier	**Het KvK nummer van de hoofdopdrachtnemer.** *(ALTIJD)* *Toelichting: dit is een invulinstructie voor de Opdrachtnemer*
Kwaliteits-regime	**IMBRO** *(ALTIJD)*
Kader aanlevering	**<Vul het inwinkader in>** *(PROJECTSPECIFIEK)* *Toelichting: Rijkswaterstaat kiest in welk kader de onderzoeken zijn uitgevoerd; keuze uit:* *a. Opdracht publieke taakuitvoering,* *b. Rechtsgrond Waterwet.*
Kader inwinning	**Invullen door diegene die de opdracht verstrekt tot het onderzoek naar de ondergrond. Keuze uit 7 opties.** *Toelichting: indien de uitvoerder van het onderzoek naar de ondergrond niet zelf verantwoordelijk is voor het bepalen welke onderzoeken naar de ondergrond nodig zijn in het licht van de werkzaamheden, kan het zo zijn dat de uitvoerder niet weet wat het doel is van het onderzoek dat hij uitvoert. Dit dient dan te worden voorgeschreven. Keuze uit onderzoek met als doel:* *1. eigenschappen van de ondergrond rondom waterkeringen te verkennen,* *2. eigenschappen van de ondergrond rondom bouwwerken en constructies te verkennen,* *3. eigenschappen van de ondergrond rondom wegen, spoorwegen, fiets- en voetpaden te verkennen,* *4. eigenschappen van de ondergrond in waterwegen te verkennen,* *5. eigenschappen van de ondergrond te verkennen met een milieu hygiënische (natuurlijke of niet natuurlijke) achtergrond,* *6. om veranderingen in de ondergrond t.g.v. werkzaamheden te verkennen. Betreffend onderzoek heeft veelal een lokaal karakter. Vaak is voorafgaand aan de werkzaamheden al in een ander kader informatie ingewonnen om de verandering te kunnen beoordelen,* *7. onderzoek met als doel een vergunning te onderbouwen.*
Eigenaar	**Invullen door diegene die opdracht geeft tot het meten van grondwater met behulp van een grondwater-monitoringput die niet in eigendom is van Rijkswater-**

	staat. *Toelichting: het kan bijvoorbeeld gaan om het tijdelijk gebruiken van een put van een ander, maar ook op grond van een burger (laten) aanleggen van een put.* *De eigenaar moet gespecificeerd worden o.b.v. KVK-nummer. In het geval dat Rijkswaterstaat eigenaar is, moet KVK-nummer 27364178 worden ingevuld.*
Onderhoudende instantie	**<Vul het KvK-nummer in>** *(PROJECTSPECIFIEK)* **Invullen door Rijkswaterstaat in geval dat grondwatermonitoringputten zullen worden aangelegd door de Opdrachtnemer maar het onderhoud door een ander wordt uitgevoerd, en die Opdrachtnemer geen kennis heeft van onderhoudende instantie(s) die hiervoor zijn gecontracteerd.** *Toelichting: de onderhoudende instantie moet gespecificeerd worden o.b.v. KvK-nummer.*
Initiële functie	**Invullen door diegene die opdracht geeft tot het aanleggen van een grondwatermonitoringput. Keuze uit 5 opties:** *Toelichting: keuze uit:* *1. Brandput,* *2. Monitoring grondwaterstand,* *3. Monitoring grondwatersamenstelling,* *4. Monitoring grondwaterstand en grondwatersamenstelling,* *5. Grondwateronttrekking.*

Vertrouwelijkheid: RWS INFORMATIE

Bijlage X Richtlijnen voor inspectie en onderhoud van faunavoorzieningen bij wegen 2008.



Bijlage Y Quick Reference Card Wekelijkse Rapportage

Wordt aan de Opdrachtnemer verstrekt na opdracht.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage Z Inspectie waterkeringen in het kader van de Zorgplicht Waterveiligheid

Zie separate documenten.

Bijlage AA Verkeersmanagement voor werk in uitvoering op Rijkswegen

Zie separaat document.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage AB Specificatie Functionele Inspecties en Testen

Zie separaat document.

Bijlage AC FIT_Typical (Generieke FIT-lijst)

Zie separaat document

Vertrouwelijkheid: RWS INFORMATIE

Bijlage AD Specificatie NEN3140 en NEN3840 inspecties

Zie separate documenten.

Bijlage AE Faaldefinitiecategorieën

Zie separaat document.

Vertrouwelijkheid: RWS INFORMATIE

Bijlage AF Industriële automatisering

Zie separate documenten.