BIJLAGE Bestek Proceseisen Cybersecurity

Inhoudsopgave

Doel bestek proceseisen Cybersecurity

Het voorliggende document is het bestek proceseisen Cybersecurity. Dit deel beschrijft de eisen op welke wijze de gevraagde Cybersecurity maatregelen geleverd moeten worden.

De eisen zijn ingedeeld naar een aantal cybersecurity onderwerpen, herkenbaar in de verschillende hoofdstukken. Voor de eenduidigheid zijn eisen voorzien van een ID-nummer bestaande uit:

1. twee beginletters 'CS' die aangeven dat deze eisen betrekking hebben op cybersecurity;
2. na de dash volgen twee of drie letters, die duiden op het cybersecurity onderwerp waarop de eis betrekking heeft;
3. een volgnummer.

ID-nummer	Omschrijving eis / bepaling
XX100	*De Opdrachtnemer dient …*

Naast de eisen zijn er bepalingen opgenomen waaruit niet direct een verplichting voortvloeit voor de Wederpartij anders dan dat de Wederpartij rekening dient te houden met wat is bepaald. Het identificatienummer wordt dan voorafgegaan door "B-" van "Bepaling".

2.2 Cybersecurity - Logische toegang (LT)

B-CS-LT010	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het Cybersecurityplan door de Wederpartij. *Toelichting: Hier wordt het Cybersecurityplan bedoeld, welke door de Wederpartij zelf wordt opgesteld conform eis:* CS-BO020
CS-LT020	De Wederpartij dient periodiek, conform de wachtwoordenrichtlijn, de wachtwoorden van alle functionele accounts van de bovenlaag van het bedienings- en besturingssysteem HIJK te wijzigen. *Toelichting: de toe te passen wachtwoorden worden door de beheerder uitgegeven.*
CS-LT030	De Wederpartij dient de wachtwoorden van alle accounts voor de logische toegang van de onderlaag van het bedienings- en besturingssysteem HIJK, conform de wachtwoordenrichtlijn, te wijzigen in de volgende situaties: 1. Na incidenten; 2. Na wijzigingen team van de Wederpartij; 3. Op verzoek van de beheerder. Zie ook eis: CS-LT110. *Toelichting: de toe te passen wachtwoorden worden door de beheerder uitgegeven.*
CS-LT040	De Wederpartij dient voor het periodiek wijzigen van de wachtwoorden een procedure op te stellen met minimaal de volgende inhoud: • Frequentie van het wijzigen per account;

	• De wijze van informeren van de gebruikers; • Waarborging continuïteit van de bediening en besturing; • Verantwoordelijkheden en bevoegdheden; • Schematische weergave van het wijzigingsproces. De procedure dient de Wederpartij met de beheerder en bediening af te stemmen en na akkoord deze te implementeren.
CS-LT050	De Wederpartij dient erop toe te zien dat: • de toegang voor de medewerkers van de Wederpartij en zijn onderaannemers tot het bedienings- en besturingssysteem HIJK uitsluitend plaatsvindt als dit strikt noodzakelijk is; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt 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 door de Wederpartij geautoriseerd zijn; • bij misbruik van accounts en autorisaties disciplinaire maatregelen worden genomen.
CS-LT060	De Wederpartij dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze verstrekt zijn, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.
CS-LT070	De Wederpartij en zijn onderaannemers dienen hun accountgegevens strikt geheim te houden, 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 of gebruikersgroep.
CS-LT080	De toegangsrechten van alle medewerkers van de Wederpartij en zijn onderaannemers dienen jaarlijks door de Wederpartij beoordeeld en geactualiseerd te worden in een formeel proces.
CS-LT090	De lokale logische toegang voor medewerkers van de Wederpartij en zijn onderaannemers tot het bedienings- en besturingssysteem HIJK inclusief de lokale objectnetwerken dient bij de hiertoe door de Wederpartij verantwoordelijk gestelde en gemandateerde medewerker/functionaris aangevraagd en goedgekeurd te worden.
CS-LT100	De Wederpartij dient de wachtwoordrichtlijn conform bijlage 004 "Wachtwoord Richtlijn" en bijlage 003 "Factsheet Wachtwoorden" voor de logische toegang tot het bedienings- en besturingssysteem HIJK in acht te nemen, voor zover dit wordt ondersteund door deze systemen. *Toelichting: systeembeperkingen dienen gerapporteerd te worden.*
CS-LT110	De Wederpartij dient van het bedienings- en besturingssysteem HIJK inclusief netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van RWS, voor zover dit ondersteund wordt door het betreffende systeem. *Toelichting: systeembeperkingen dienen gerapporteerd te worden.*
CS-LT120	De Wederpartij dient de werkzaamheden aan: 1. Installatietekeningen; 2. beveiligings- en veiligheidsdocumentatie en -instructies;

	van: a. het kunstwerk HIJK; b. bediengebouwen en -ruimten; c. het bedienings- en besturingssysteem HIJK; d. kabels en leidingen; dan wel de werkzaamheden: 3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten; 4. aan het bedienings- en besturingssysteem HIJK zelf; 5. aan kabels en leidingen; door medewerkers te laten verrichten, die een geheimhoudingsverklaring hebben ondertekend en over een Verklaring Omtrent het Gedrag (VOG) beschikken, die gerelateerd is aan de beoogde Prestatie.
CS-LT130	De Wederpartij dient te zorgen voor een procedure en actuele registratie van: • de fysieke toegang van de medewerkers en onderaannemers tot ICT en IA gerelateerde ruimten; • de door de Wederpartij aan alle medewerkers en onderaannemers verstrekte accounts met bijbehorende autorisatie voor de logische toegang tot het bedienings- en besturingssysteem HIJK.
CS-LT140	De Wederpartij dient een voorstel te maken voor de benodigde functionele accounts van het bedienings- en besturingssysteem HIJK, vervolgens dit voorstel af te stemmen met de beheerder en na akkoord te implementeren.
CS-LT150	De Wederpartij dient tijdens de contractduur de rechten van accounts op verzoek van beheerder aan te passen. *Toelichting: Ga uit van maximaal 5 verzoeken tijdens de totale contractduur.*

2.3 Cybersecurity - Incidenten en Response Plan (IRP)

CS-IRP010	De Wederpartij dient Cybersecurity incidenten (zowel fysiek als digitaal) direct te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een cybersecurity incident bij het onmiskenbaar worden van een (dreigend of reeds opgetreden) cybersecurity risico als gevolg van een (mogelijke) overtreding van het Cybersecurity beleid of onregelmatigheid. Voorbeelden van cybersecurity incidenten zijn: • verlies van functie, apparatuur of voorzieningen; • systeemstoringen of overbelasting door opzet; • menselijke fouten met opzet 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, waaronder zelf aangelegde netwerkkoppelingen; • niet-naleving van beleid of gedragsregels; • virusmeldingen; • verlies of diefstal van bedrijfsmiddelen; • oneigenlijk gebruik van bevoegdheden;

	• vandalisme, moedwillige beschadiging.
CS-IRP020	De Wederpartij dient een geborgde procedure op te stellen en te implementeren die regelt dat zijn medewerkers Cybersecurity incidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de Missie Kritische Ondersteuning (MKO) van Opdrachtgever. En dat de Wederpartij alle Cybersecurity incidenten, verdachte of zwakke plekken in systemen of diensten registreert middels het cybersecurity registratie template en deze rapporteert aan de beheerder.
CS-IRP030	Ten behoeve van het rapporteren en registreren dient de Wederpartij een Cybersecurity registratie template op te stellen en deze af te stemmen met de Opdrachtgever.
CS-IRP040	De Wederpartij dient een sleutelfunctionaris te benoemen die verantwoordelijk is voor de Prestatie met betrekking tot Cybersecurity.
CS-IRP050	De Wederpartij draagt zorg voor aansluiting en borging van het eigen Cybersecurity incidentmanagementproces op die van RWS, zie bijlage 030.
CS-IRP060	Indien er sprake is van cybersecurity inbreuken of verhoogde dreiging, dient de Wederpartij de richtlijn CS R03 Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging conform bijlage 028 te volgen.
CS-IRP070	De Wederpartij dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.
CS-IRP080	De Wederpartij dient een geborgde procedure op te stellen voor cybersecurity incidentrespons ingeval van cybersecurity incidenten en de daaruit voortvloeiende calamiteiten.
CS-IRP090	De Wederpartij dient jaarlijks de cybersecurity incident responseplannen te beproeven aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven en de bijbehorende resultaten ter kennis te brengen van de Opdrachtgever.
CS-IRP100	Opdrachtgever kan jaarlijks onaangekondigd een PEN-test uitvoeren. De hieruit voortvloeiende onvolkomenheden, welke onderdeel zijn van de Opdracht, dienen door de Wederpartij opgepakt te worden.
CS-IRP110	De Wederpartij dient ten minste één keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de rapportage ter informatie aan te leveren bij Opdrachtgever.
CS-IRP120	De Wederpartij dient aan te geven welke ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen, die het bedienings- en besturingssysteem HIJK kan genereren en hoe deze geactiveerd en benut kunnen worden voor registratie, rapportage en analyse van Cybersecurity incidenten, vervolgens dit voorstel af te stemmen met Opdrachtgever en na akkoord te implementeren.

2.4 Cybersecurity – Netwerkkoppelingen (NK)

CS-NK010	De Wederpartij dient ervoor te zorgen dat er geen (Rechtstreekse) toegang tot het bedienings- en besturingssysteem HIJK vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail – , een kantoornetwerk of een zelf aangelegd netwerk mogelijk is.
CS-NK020	Het koppelen van mobiele apparatuur van derden of portable 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 Opdrachtgever.
CS-NK030	De Wederpartij dient alleen mobiele datadragers toe te passen die door de beheerder zijn vrijgegeven.
CS-NK040	De Wederpartij dient de Prestatie zodanig te verrichten, dat geen internet, draadloze voorzieningen (Wifi, GPRS/UMTS etc.) of inbelvoorzieningen worden gekoppeld aan het besturings- en bediensysteem HIJK.
CS-NK050	De Wederpartij dient bij koppeling van randapparatuur aan de ICT en/of IA van de Opdrachtgever de richtlijn CS R02 Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen van RWS conform bijlage 028 "Richtlijnen Cybersecurity' aan te houden voor bescherming tegen malware.
CS-NK060	De Wederpartij draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door het aanleveren van deze configuratiegegevens aan Opdrachtgever na vernieuwing/wijziging. *Toelichting: De CMDB wordt door de beheerder beheerd.*

2.5 Cybersecurity - malware, hardening en patching (MHP)

CS-MHP010	De Wederpartij dient met een voorstel te komen voor de wijze waarop detectie van en preventie tegen malware plaats kan vinden, zonder negatieve consequenties voor de faalkans en performance van het bedienings- en besturingssysteem HIJK. Het voorstel dient de Wederpartij vervolgens met de Opdrachtgever af te stemmen en na akkoord te implementeren en vast te leggen in een geborgde procedure.
CS-MHP020	De Wederpartij dient met een voorstel te komen welke hardenings mogelijkheden het bedienings- en besturingssysteem HIJK en het lokale objectnetwerk biedt en welke consequenties en risico's elk van deze hardeningsmaatregel met zich meebrengt voor het functioneren van de HIJK. Het voorstel dient de Wederpartij vervolgens met de Opdrachtgever af te stemmen en na akkoord te implementeren. Denk hierbij aan: • niet noodzakelijke datanetwerkservices uit te zetten; • niet noodzakelijke processen/services voor de bediening en besturing om HIJK uit te zetten; • het verwijderen (patchen) van bekende kwetsbaarheden; • alle poorten (USB/IP/..) 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.
CS-MHP030	De Wederpartij dient over een geborgde procedure te beschikken voor het borgen van de hardening van het bedienings- en besturingssysteem van de HIJK.
CS-MHP040	De Wederpartij dient een procedure te hebben voor het beoordelen van een (spoed)patch met behulp van een risicoanalyse voor wat betreft de impact op het bedienings- en besturingssysteem van de HIJK, inclusief het Test en OntwikkelSysteem.
CS-MHP050	De Wederpartij dient op basis van de beoordeling, zoals bedoeld in CS-MHP040, de Opdrachtgever per patch een implementatieadvies ter Acceptatie voor te leggen. Daarbij gelden de volgende doorlooptijden: • voor kritieke patches: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag; • voor niet-kritieke patches: maximaal twee maanden na melding door de Opdrachtgever.
CS-MHP060	De Wederpartij dient de patches, na Acceptatie van het implementatieadvies door de Opdrachtgever, conform het (aangepaste) advies te implementeren.
CS-MHP070	De Wederpartij dient, na signalering van technische kwetsbaarheden in het bedienings- en besturingssysteem van de HIJK inclusief ondersteunende netwerken, passende mitigerende maatregelen te nemen om de risico's van de kwetsbaarheden te minimaliseren en dit te borgen middels een procedure, waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijnde doorlooptijden.
CS-MHP080	De Wederpartij dient bij patches en anti-virusupdates, die vanaf Internet worden gedownload, aantoonbaar te kunnen maken dat deze vanaf een betrouwbare bron afkomstig zijn.
CS-MHP090	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging door de Wederpartij schriftelijk te worden vastgelegd voorzien van een

	risicoafweging.
CS-MHP100	De Wederpartij 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.
CS-MHP110	De Wederpartij dient het mogelijk inzetten van Antimalware voorzieningen eerst met de beheerder af te stemmen alvorens deze ingezet mogen worden.
CS-MHP120	Onderstaande eisen zijn ook van toepassing op het Test en OntwikkelSysteem (TOS). CS-MHP010 CS-MHP040 CS-MHP050 CS-MHP060 CS-MHP080 CS-MHP090 CS-MHP100 CS-MHP110

2.6 Cybersecurity - Bewustwording en Training (BT)

CS-BT010	De Wederpartij en al zijn onderaannemers zijn verplicht om de door Opdrachtgever beschikbaar gestelde periodieke Cybersecurity Awareness training en de E-Learning modulen te volgen en hiernaar te handelen.
CS-BT020	Iedere medewerker van de Wederpartij, inclusief zijn onderaannemers, dient zich bewust te zijn van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en te weten dat gebruikers- en systeemactiviteiten worden gelogd.
CS-BT030	De Wederpartij en zijn onderaannemers dienen aan sociale controle te doen, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden m.b.t. cybersecurity in het periodieke werkoverleg met het eigen management/Objectbeheerder.
CS-BT040	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 beheerder.
CS-BT050	De Wederpartij inclusief onderaannemers, dienen bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties in het kader van cybersecurity, deze te melden bij de SWD. En in afstemming met de SWD handelingen te verrichten of maatregelen te treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken, zolang dit niet ten koste gaat van de beschikbaarheid.
CS-BT060	De Wederpartij, inclusief onderaannemers, dienen zorgvuldig om te gaan met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
CS-BT070	Voor de Wederpartij, inclusief onderaannemers, is toegang tot internet en het gebruik van email vanaf het bedienings- en besturingssysteem HIJK en overige

	daaraan ondersteunende IA-systemen strikt verboden.
CS-BT080	Bij het constateren van onregelmatigheden in de logische toegang tot het bedienings- en besturingssysteem HIJK dient de Wederpartij inclusief onderaannemers, dit onverwijld als een cybersecurity incident te melden bij de beheerder.
CS-BT090	Het is de Wederpartij strikt verboden om ongeautoriseerd portable apparatuur of usb-sticks aan het bedienings- en besturingssysteem HIJK inclusief het netwerk of aan- of af te koppelen. Alleen de door de beheerder beschikbaar gestelde gegevensdragers dienen gebruikt te worden.
CS-BT100	Alleen geautoriseerde medewerkers van de Wederpartij is het na goedkeuring van de beheerder toegestaan om systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur te koppelen aan het bedienings- en besturingssysteem HIJK inclusief het lokale netwerk, mits er geen externe verbindingen vanaf deze systemen toegepast kunnen worden.
CS-BT110	Gegevensdragers dienen door de Wederpartij altijd vooraf op malware gecontroleerd te worden voordat deze worden gekoppeld aan het bedienings- en besturingssysteem HIJK, Test en OntwikkelSysteem (TOS) of overige ondersteunende IA-systemen en netwerken.
CS-BT120	De Wederpartij dient cybersecurity incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces te melden bij de beheerder.
CS-BT130	De Wederpartij dient onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces te melden bij de beheerder.
CS-BT140	De Wederpartij, inclusief onderaannemers, dienen ervoor te zorgen dat onbeheerde systemen van het bedienings- en besturingssysteem HIJK – zo mogelijk - worden gelocked.
CS-BT150	De Wederpartij dient er zorg voor te dragen en op toe te zien dat hun medewerkers en onderaannemers: • de periodieke Cybersecurity trainingen en E-Learningmodulen volgen en een actuele administratie hiervan bijhouden; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen van het bedienings- en besturingssysteem HIJK en overige ondersteunende IA-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel. De beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; • ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; • alle bedrijfsmiddelen, systeemdocumentatie van het bedienings- en besturingssysteem HIJK en overige ondersteunende IA-systeemdocumentatie van RWS die ze in hun bezit hebben retourneren bij beëindiging van het , contract of overeenkomst; • dat de toegangsrechten en verstrekte toegangsmiddelen van alle medewerkers direct worden geblokkeerd dan wel ingeleverd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • worden geïnformeerd over de calamiteitenplannen en testactiviteiten; • De centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau correct gebruiken.
CS-BT160	De Wederpartij bespreekt en evalueert in de periodieke werkoverleggen met Opdrachtgever de Cybersecurity incidenten 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.
CS-BT170	De Wederpartij ziet erop toe dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging zoals fysieke en logische toegang en melding van Cybersecurity incidenten.
CS-BT180	De Wederpartij dient te waarborgen dat alle informatie van RWS, die tijdens de werkzaamheden op eigen apparatuur terecht zijn gekomen na beëindiging van de Prestatie/Overeenkomst aantoonbaar vanaf de betreffende apparatuur verwijderd is.

2.7 Cybersecurity - gecontroleerd wijzigen (GW)

CS-GW010	De Wederpartij dient over een geborgde procedure te beschikken voor het (laten) inventariseren, registreren en actualiseren van alle Configuration Items (CI's) van het bedienings- en besturingssysteem van de HIJK met bijbehorende settings/configuraties en deze aan Opdrachtgever te verstrekken, zodat Opdrachtgever instaat gesteld wordt om de Configuration Management Database (CMDB) actueel te houden.
CS-GW020	De Wederpartij dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen, inclusief updates en patches, aan het bedienings- en besturingssysteem van de HIJK, inclusief de beveiliging- en netwerkomgeving en het Test en OntwikkelSysteem, die aansluit op de bestaande procedures van de beheerder en Opdrachtgever. Alle wijzigingen dienen conform de wijzigingsprocedure te worden geregistreerd.
CS-GW030	Voor wijzigingen aan het bedienings- en besturingssysteem van de HIJK dient door de Wederpartij altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten voordat uitvoering van werkzaamheden plaatsvindt zijn goedgekeurd door de beheerder.
CS-GW040	De Wederpartij dient jaarlijks de settings/configuraties van het bedienings- en besturingssysteem van de HIJK zoals vermeld in de CMDB te vergelijken met de daadwerkelijke situatie in het veld en dient de CMDB indien nodig bij te werken.
CS-GW050	Wijzigingen in het bedienings- en besturingssysteem van de HIJK dienen, indien mogelijk, voorafgaand aan de implementatie in de productieomgeving te worden getest in een testomgeving (bv de TOS) om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit van het systeem of beveiliging van de organisatie. Indien haalbaar moet voor het bedienings- en besturingssysteem van de HIJK controle worden uitgevoerd voor de authenticiteit/integriteit van de software en het vrij zijn van malware voorafgaande aan de implementatie op operationele systemen.
CS-GW060	De Wederpartij dient zorg te dragen voor en erop toe te zien dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebracht als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en dat de benodigde informatie voor het actualiseren van de CMDB bij de Opdrachtgever wordt aangeleverd.

CS-GW070	De Wederpartij dient voor elke wijziging een terugval scenario op te stellen 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.
CS-GW080	De Wederpartij dient erop toe te zien dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging op te leveren.
CS-GW090	De Wederpartij dient alle Configuratie Items met bijbehorende settings/configuraties na wijzigingen door te geven aan Opdrachtgever, zodat de CMDB actueel kan worden gehouden.
CS-GW100	Opdrachtgever stelt een Test en OntwikkelSysteem ter beschikking. Indien dit niet toereikend is om de gewenste testen uit te voeren, dient de Wederpartij zelf te voorzien in aanvullende testvoorzieningen.

2.8 Cybersecurity - beheer en onderhoud (BO)

CS-BO010	De Wederpartij dient de Prestatie zodanig te verrichten, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.
CS-BO110	De Wederpartij dient zorg te dragen voor en erop toe te zien dat cybersecurity incidenten in de breedste zin van het woord geen kans krijgen om een negatieve invloed uit te oefenen op de huidige faalkans en beschikbaarheid van het object.
CS-BO020	De Wederpartij dient een plan "Cybersecurity" op te stellen als uitwerking van de cybersecurityeisen waarbij de inhoud ten minste de onderdelen met betrekking tot het Meerjarig Onderhoud bevat uit: 1. Paragraaf 2.8 Cybersecurity – beheer en onderhoud; 2. de Template Plan Cybersecurity, opgenomen in bijlage 023.
CS-BO030	De Wederpartij dient zorg te dragen voor het evalueren van risico's en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cycle management.
CS-BO040	De Wederpartij dient ten minste jaarlijks de maatregelen voor cybersecurity te monitoren te meten en waar nodig verbetermaatregelen te treffen.
CS-BO050	De Wederpartij dient ervoor te zorgen dat alle eisen voor de Wederpartij in de beheer en onderhoudscontracten met onderaannemers worden geborgd, zodat zowel de Wederpartij als zijn onderaannemers aan de gestelde eisen in het contract voldoen.
CS-BO060	De Wederpartij dient waar nodig zorg te dragen voor en erop toe te zien dat in SLA/DAP afspraken met Opdrachtgever en onderaannemers worden gemaakt, waarbij rekening wordt gehouden met de beschikbaarheid en de faalkans van de HIJK, over tenminste: • De dienstverlening en functionaliteit; • Tijd van openstelling, bereikbaarheid en reactietijd, Cybersecurity incident melding en afhandeling; • Wat wordt verstaan onder een storing, Cybersecurity incident en zwakke plek; • Het classificeren van Cybersecurity 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 Cybersecurity incidenten; • Noodprocedures met zowel interne als externe leveranciers van het bedienings- en besturingssysteem HIJK; • 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 Cybersecurity incidenten 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.

CS-BO070	De Wederpartij dient zorg te dragen voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor het bedienings- en besturingssysteem van de HIJK alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen na een (software) wijziging.
CS-BO080	De Wederpartij dient de Documenten met betrekking tot het bedienings- en besturingssysteem van de HIJK te beveiligen tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.
CS-BO090	De Wederpartij dient voor de beveiliging van informatie van de Opdrachtgever en Documenten de door de Opdrachtgever aangegeven documentclassificatie en bijbehorende beveiligingsmaatregelen aan te houden conform richtlijn CS R01 Richtlijn voor omgaan met vertrouwelijke informatie en documenten conform bijlage 028 "Richtlijnen Cybersecurity".
CS-BO100	De Wederpartij dient zorg te dragen voor een geborgde procedure die de personele toegang van zijn medewerkers, voorafgaand aan de uitvoering van werkzaamheden regelt, die aansluit op de procedure van de beheerder, conform bijlage 029 'Huisregels HIJK" onder hoofdstuk 3.
CS-BO110	De Wederpartij 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.
CS-BO120	Voor de fysieke toegang tot objecten en de ruimten hierbinnen dient de Wederpartij het sleutelplan van de beheerder op te volgen.

2.9 Cybersecurity - Back-ups (BU)

CS-BU010	De Wederpartij dient na afronding van de uitvoeringswerkzaamheden te voorzien in een back-up van het bedienings- en besturingssysteem van de HIJK conform de huidige back-up procedure, zie bijlage 026b/c en deze te overhandigen aan de beheerder.
CS-BU020	De Wederpartij dient de huidige gedocumenteerde herstelprocedures, zie bijlage 026d, daar waar nodig te actualiseren.
CS-BU030	De Wederpartij dient de huidige voorzieningen voor het back-up en restoreproces te beoordelen en indien nodig verbeteringen in overleg met de Opdrachtgever uit te voeren.

2.10 Cybersecurity - Logging en Monitoring (LM) (Optioneel)

CS-LM010	De Wederpartij dient met een voorstel te komen welke data aanvullend op eis HIJK-BB-F-12 gelogd moet worden om cybersecurity incidenten te kunnen analyseren en welke beveiligingsspecifieke logsystemen daarvoor nodig zijn. Het voorstel dient de Wederpartij vervolgens met de Opdrachtgever af te stemmen en na akkoord te implementeren.
CS-LM020	De Wederpartij dient er voor te zorgen en op toe te zien dat: • de loggegevens van het bedienings- en besturingssysteem HIJK in een of meerdere aparte bestanden worden weggeschreven en opgeslagen die alleen toegankelijk zijn voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van het bedienings- en besturingssysteem HIJK inclusief netwerkelementen beschermd worden tegen verlies of wijziging; • de logbestanden drie maanden bewaard worden; • loggegevens die gebruikt worden voor cybersecurity incidentonderzoeken worden veiliggesteld op locatie en conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
CS-LM020	De Wederpartij dient voor de levering van logbestanden aan derden expliciet toestemming te hebben van de beheerder.
CS-LM030	De Wederpartij dient in het kader van de Algemene verordening gegevensbescherming (AVG) de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens (waaronder camerabeelden) rechtmatig te behandelen.
CS-LM040	Indien de Wederpartij persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens (waaronder camerabeelden) opslaat en/of verwerkt, dient de Wederpartij een verwerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon “RWS Verwerkersovereenkomst”, die na gunning, op verzoek van de Wederpartij beschikbaar wordt gesteld.