Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

Cybersecurity Implementatierichtlijn Objecten

Datum	23 april 2021
Versie	2.4
Status	Definitief

Colofon

Uitgegeven door	CIV/IRN/Security Centre/Security by Design
Auteurs	Turabi Yildirim Mark van Leeuwen Michael Theuerzeit Mieke van Nierop
Datum	23 april 2021
Versie	2.4
Status	Definitief

Versiebeheer en wijzigingshistorie
Het beheer van dit document berust bij Rijkswaterstaat CIV/IRN/Security Centre/Security by Design.

2.0	18-04-2021	RWS interne versie CSIR
2.4	23-04-2021	Gestripte versie t.b.v. aanbestedingen

Over Rijkswaterstaat
Rijkswaterstaat is de uitvoeringsorganisatie van het ministerie van Infrastructuur en Waterstaat en werkt dagelijks aan een veilig, leefbaar en bereikbaar Nederland.
We willen leven in een land dat beschermd is tegen overstromingen. Een land waar voldoende groen is, en voldoende en schoon water. En waar we vlot en veilig van A naar B kunnen.
Daarvoor zetten de mensen van Rijkswaterstaat zich dagelijks in. Met ruim 200 jaar kennis van de inrichting van ons land weten ze dat dit meer is dan het technisch uitvoeren van projecten aan weg en water. Het gaat ook om de balans tussen al die belangen: economie, milieu, woongenot.

Rechten en vrijwaring
Rijkswaterstaat is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan Rijkswaterstaat geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. Rijkswaterstaat aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Inhoudsopgave

1 INLEIDING 4
1.1 BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO) EN DE IEC 62443 4
1.2 CYBERSECURITY IMPLEMENTATIERICHTLIJN OBJECTEN (CSIR) 6
1.3 INSTRUCTIE VOOR PRAKTISCHE TOEPASSING 10
1.4 INHOUD 11
2 VERDIEPENDE MAATREGELPAKKETTEN 12
2.1 MAATREGELEN FYSIEKE TOEGANGSBEVEILIGING IA-GERELATEERDE RUIMTEN 12
2.2 MAATREGELEN LOGISCHE TOEGANG 16
2.3 MAATREGELEN BEVEILIGINGSINCIDENTEN EN INCIDENT RESPONSE PLAN 19
2.4 MAATREGELEN NETWERKKOPPELINGEN EN CRYPTOGRAFIE 21
2.4.1 NETWERKKOPPELINGEN 21
2.4.2 CRYPTOGRAFIE 23
2.5 MAATREGELEN BESCHERMING TEGEN KWETSBAARHEDEN 24
2.5.1 ANTI-MALWARE 24
2.5.2 HARDENING 25
2.5.3 PATCHING 26
2.6 MAATREGELEN LOGGING EN MONITORING 28
2.7 MAATREGELEN BEWUSTWORDING EN TRAINING 32
2.7.1 MEDEWERKERS 32
2.7.2 MANAGERS 35
2.8 MAATREGELEN GECONTROLEERD WIJZIGEN 37
2.9 MAATREGELEN BEHEER EN ONDERHOUD 39
2.10 MAATREGELEN BACK-UPS 42

BIJLAGE CSR 1 OMGAAN MET VERTROUWELIJKE INFORMATIE EN DOCUMENTEN 44
BIJLAGE CSR 2 PERSONELE TOEGANG 47
BIJLAGE CSR 3 ARCHITECTUUR OBJECTNETWERK 48
BIJLAGE CSR 4 HET VEILIG KOPPELEN VAN BEHEER- EN ONDERHOUDSAPPARATUUR AAN ICT- EN IA-SYSTEMEN 51
BIJLAGE CSR 5 DRAADLOZE NETWERKEN 53
BIJLAGE CSR 6 IOT 54
BIJLAGE CSR 7 WACHTWOORDEN 56
BIJLAGE CSR 8 PATCH MANAGEMENT 59
BIJLAGE CSR 9 HARDENING 64
BIJLAGE CSR 10 LOGGING 66
BIJLAGE CSR 11 MALWARE SCANNING EN OPSCHONING MIDDELS EEN USB 68
BIJLAGE CSR 12 CONTINUÏTEITSPLAN VOOR ENERGIEVOORZIENING 71
BIJLAGE CSR 13 HANDELSWIJZE BIJ SOC INCIDENT MELDING EN VERHOOGDE DREIGING 72
BIJLAGE CSR 14 INCIDENT RESPONSE 77
BIJLAGE CSR 15 RECOVERYPLAN 83
BIJLAGE CSR 16 REGISTRATIE ASSETS IN EEN CONFIGURATIEMANAGEMENT DATABASE (CMDB) 89
BIJLAGE CSR 17 BEVEILIGINGSHUISREGELS 119
BIJLAGE CSR 18 BACK-UP EN RECOVERY 120
BIJLAGE CSR 19 INTELLECTUEEL EIGENDOM 121
BIJLAGE CSR 20 CAMERA'S EN OMGANG MET CAMERABEELDEN VAN DE VERKEERSREGISTRATIESYSTEMEN 128
BIJLAGE CSR 21 UNIFORM AANLEVEREN VAN INCIDENTRAPPORTAGES 129
BIJLAGE CSR 22 VIRTUALISATIE 131
BIJLAGE CSR 23 VERWIJDERING EN VERNIETIGING VAN INFORMATIE EN APPARATUUR 132
BIJLAGE A BEGRIPPENLIJST 133
BIJLAGE B CYBERSECURITY DOSSIER / CYBERSECURITY BEVEILIGINGSPLAN 135
BIJLAGE C BEST PRACTICE VOOR RISICO INSCHATTING BIJ CSIR AFWIJKINGEN 136

1 Inleiding

De samenleving verandert snel onder invloed van technologie en digitalisering. Digitalisering is de belangrijkste bron van groei, innovatie en nieuwe bedrijvigheid. In de informatiesamenleving ontstaan nieuwe kansen door de digitalisering. Tegenover de kansen van digitalisering staan bedreigingen op het gebied van cybersecurity. Cybercrime, cyberspionage en cybersabotage kunnen systemen en processen verstoren, met grote gevolgen voor de volksgezondheid, veiligheid en economie. Deze digitale bedreigingen vragen van de partners in vitale sectoren met bijbehorende vitale processen om een gezamenlijke aanpak en inspanning.

De komende jaren kan verdere digitalisering van de productieprocessen verwacht worden en daarmee ook de grotere afhankelijkheid van ICT en Industriële Automatisering (IA) in onze samenleving. Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaatsvindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Industriële Automatisering draagt ook zorg voor het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen). Productieprocessen waarvan sommige vitaal zijn stellen eisen aan de betrouwbaarheid en beschikbaarheid en zijn digitaal vaak verbonden met processen van ketenpartners waarmee samengewerkt wordt. Voor een effectieve en efficiënte samenwerking is de beveiliging van de Industriële Automatisering dan ook essentieel.

Industriële Automatisering zorgt er bijvoorbeeld voor dat sluizen en bruggen functioneren, energie en gas worden gedistribueerd, drinkwater wordt gereinigd, afvalwaterzuivering plaatsvindt, treinen op bestemming komen, containers worden vervoerd en liften en overige gebouwbeheersystemen functioneren. De vitale processen van organisaties worden vaak ondersteund door Industriële Automatisering en door de bescherming van Industriële Automatisering worden ook de te beschermen belangen gewaarborgd.

De doelstelling die met dit document wordt nagestreefd is de vitale infrastructuur met Industriële Automatisering cyberweerbaar te maken en te houden door het treffen en onderhouden van een passende set van beheersmaatregelen. De doelgroep voor dit document zijn objecteigenaren, objectbeheerders, assetmanagers, omgevingsmanagers, technisch managers, contractmanagers, architecten, netwerkspecialisten, staf medewerkers, IA adviseurs, IA cybersecurity adviseurs, opdrachtnemers en leveranciers.

1.1 Baseline Informatiebeveiliging Overheid (BIO) en de IEC 62443

De BIO schrijft het basisniveau voor informatiebeveiliging voor binnen de overheid. De BIO biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van de overheid.
De BIO richt zich vooral op de beveiliging van de Kantoorautomatisering (KA)
en minder op de Industriële Automatisering. Hierbij zijn Procesautomatisering (PA) en Operationele Technologie (OT) synoniemen voor Industriële Automatisering (IA).

Vergelijking Kantoorautomatisering en Industriële Automatisering
Voor de IA zijn aanvullende eisen en maatregelen nodig om de risico's in het IA domein te beheersen. Dit omdat er andere technologie en componenten worden ingezet, de dreigingen en kwetsbaarheden en de life-cycle processen verschillen. Een wezenlijk onderscheid en focuspunt tussen de kantoorautomatisering en procesautomatisering is dat binnen de BIO de focus ligt op de **informatie** en de **vertrouwelijkheid** ervan en dat binnen procesautomatisering de focus ligt op de **functies van het object of systeem/proces** en de **betrouwbaarheid** ervan. Hiernaast ligt binnen procesautomatisering ook meer focus op **safety** naast **security**. Dit verklaart ook de focus op betrouwbaarheid van Industriële Automatisering in termen van de RAMSSHEEP aspecten voor betrouwbaarheid en beschikbaarheid. Een beschikbare object- of systeemfunctie die niet veilig

(safety) is, heeft weinig toegevoegde waarde binnen de Industriële Automatisering. Een ander wezenlijk verschil is dat binnen de BIO betrouwbaarheid gedefinieerd wordt in termen van **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** met focus op informatie (afgekort **BIV**) en dat binnen procesautomatisering **betrouwbaarheid** anders wordt gedefinieerd waarbij de focus ligt op de functies van het object en/of het systeem/proces. Zie voor de definities van betrouwbaarheid en beschikbaarheid en het onderscheid hiertussen de begrippenlijst in de bijlagen. Bij Industriële Automatisering hanteert men de begrippen uit de RAMSSHEEP[1] en worden betrouwbaarheid en beschikbaarheid afzonderlijk gedefinieerd. Dit betekent dat de lading en strekking van de BIO eisen en maatregelen niet zondermeer betekenis kunnen hebben in het werkveld van Industriële Automatisering. De binnen de BIO onderkende BBN niveaus met bijbehorende BIV waarden die bedoeld zijn voor een IT/Kantooromgeving bieden dan ook weinig houvast voor de beveiliging van Industriële Automatisering. Een vertaalslag en aanvulling op de eisen en maatregelen is dan ook nodig om de BIO eisen en maatregelen betekenis en toegevoegde waarde te laten hebben voor de Industriële Automatisering.

Vergelijking normenkader BIO en IEC 62443
Voor de beveiliging van Industriële Automatisering zijn standaarden beschikbaar. De Europese standaard hiervoor is de IEC 62443. De IEC 62443 is in feite een verzameling van normen, technische rapporten en gerelateerde informatie voor het beveiligen van Industriële Automatisering. Deze documenten zijn het resultaat van het IEC proces waarbij ANSI/ISA-62443 voorstellen (vanuit de ISA99 werkgroepen) en andere bijdragen (zoals van de WIB) worden ingediend bij landelijke commissies. Aanmerkingen op een indiening worden geëvalueerd door verschillende IEC 62443 normcommissies waarbij de commentaren worden besproken en, als het nodig is, veranderingen worden doorgevoerd. De IEC ontwikkelt wereldwijde normen onder de vlag van de World Standards Cooperation, waar de ISO en ITU lid van zijn.

De BIO is voor de overheid verplicht en is een baseline. De BIO bevat generieke controls/beheersdoelen voor de IT/Kantooromgeving die ook van toepassing kunnen zijn voor Industriële Automatisering. De BIO controls/beheersdoelen moeten echter wel vertaald worden voor toepassing en betekenis binnen de Industriële Automatisering en aangevuld worden met controls/beheersdoelen om de specifieke risico’s van de Industriële Automatisering ook te kunnen mitigeren. De IEC 62443 is een standaard voor de beveiliging van Industriële Automatisering maar is niet verplicht en mist naast de BIO ook overige van toepassing zijnde controls/beheersdoelen uit andere wet en regelgeving.

In de praktijk worden vaak de datanetwerken van de Kantoorautomatisering (KA) met die van Industriële Automatisering vervlecht. Een zuivere scheidslijn is dan ook niet meer te trekken tussen de KA en die van de Industriële Automatisering. De Industriële Automatisering wordt ook nog eens vaak vanuit een KA omgeving aangestuurd en/of beheerd en onderhouden waar de BIO verplicht is en waarop aanvullende controls en maatregelen nodig zijn voor de Industriële Automatisering.

Synthese Cybersecurity Implementatierichtlijn Objecten
Gezien het verplichte karakter van de BIO, de vervlechting van de datanetwerken van KA en IA en de vereiste om zowel voor de BIO en de IEC 62443 een management systeem op te zetten en te onderhouden ligt het meer voor de hand om te komen tot een synthese product. De BIO schrijft een Information Security Management Systeem (ISMS) voor en de IEC 62443 heeft het over een Cyber Security Management Systeem (CSMS). De ontwikkeling is dat ook de IEC 62443 het begrip ISMS gaat hanteren in plaats van CSMS. Twee management systemen inrichten en erop nahouden voor een (overheid)organisatie is ondoenlijk en uitgaande van de overheidssituatie dat een overheidsorgaan altijd de kantooromgeving als thuisbasis heeft van waaruit andere activiteiten worden ontplooid, ligt het meer voor de hand om de BIO en het bijbehorende ISMS (eigenlijk het zuivere ISO 27001 framework) als basis te gebruiken voor het management systeem en deze te vullen met de relevante controls en maatregelen uit de IEC 62443 maar ook uit andere bronnen om de risico’s binnen het werkveld van IA te kunnen mitigeren.

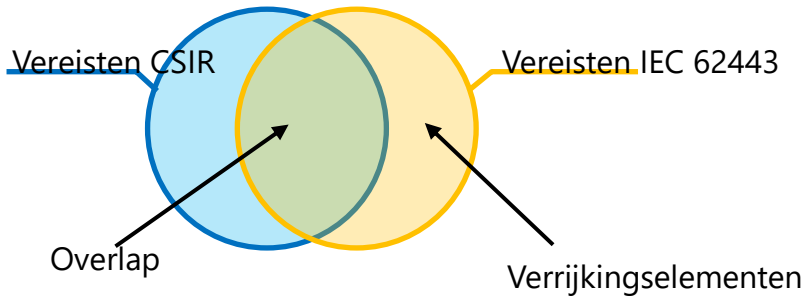
[1] RAMSSHEEP staat voor Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economics and Politics.

De eerste versie van de Cybersecurity Implementatierichtlijn Objecten van RWS was het product van deze synthese waarbij werd uitgegaan van de Baseline Informatiebeveiliging Rijkdienst 2012 (BIR 2012) als basis en de concept delen van de IEC 62443. Met de komst van de BIO en de definitief geworden delen van de IEC 62443 is de Cybersecurity Implementatie Richtlijn Objecten geactualiseerd en heeft als eerste basis de relevante BIO controls/beheersdoelen die aangevuld zijn met niet overlappende controls en requirements uit de IEC 62443 en overige bronnen. In de volgende paragraaf volgt een beschrijving hoe de synthese van Cybersecurity Implementatierichtlijn Objecten versie 2.0 tot stand is gekomen.

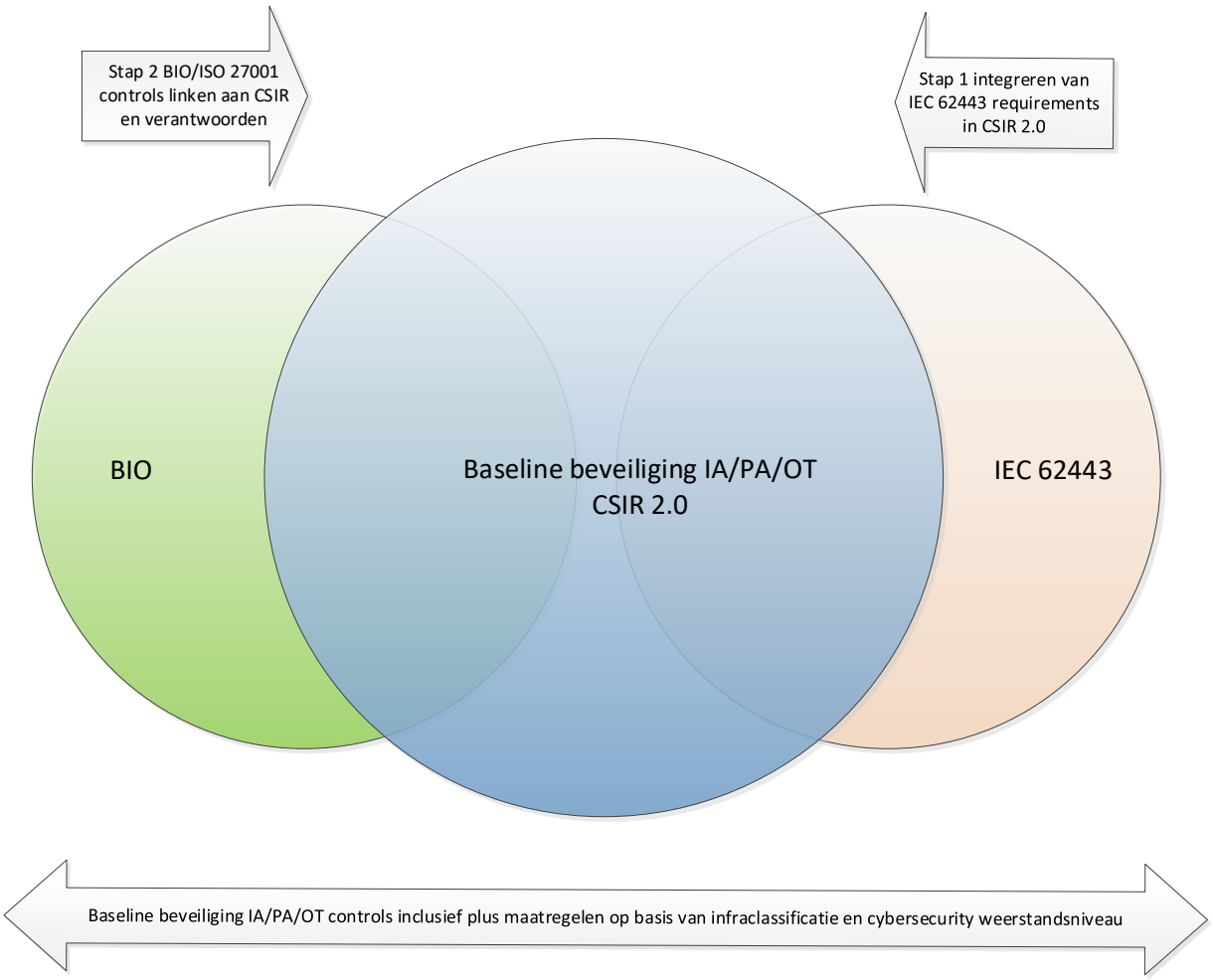
1.2 Cybersecurity Implementatierichtlijn Objecten (CSIR)

Beschrijving CSIR
De eerste versie van de Cybersecurity Implementatierichtlijn Objecten is een vertaalslag van de relevante controls/beheersdoelen uit de BIO en de NCSC Checklist beveiliging ICS/SCADA systemen met controls en requirements aanvullingen uit de relevante delen van de IEC 62443 voor de beveiliging van Industriële Automatisering. Waar nodig zijn ook aanvullingen gedaan uit overige best practices voor de beveiliging van Industriële Automatisering. De formulering van de controls/beheersdoelen heeft een operationeel karakter en is daardoor meer geschikt voor toepassing door opdrachtgevers en opdrachtnemers binnen Grond Weg en Waterbouw (GWW) projecten. Ook worden de controls/beheersdoelen geoormerkt of ze een proces of systeemtechnische vereiste betreffen opdat aansluiting wordt gevonden bij het proces van Systems Engineering inclusief de fasering van het V-model voor GWW projecten. Voor het overzicht van de proces- en systeemtechnische controls wordt verwezen naar de vraagspecificatie/contract.

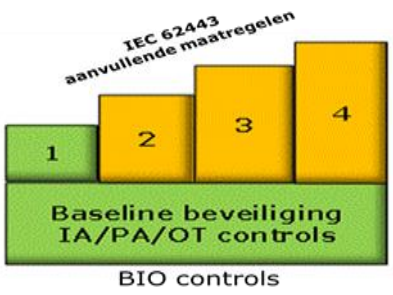
Ontwikkelproces CSIR
De Cybersecurity Implementatierichtlijn Objecten 2.0 is een doorontwikkeling van de eerste versie van de Cybersecurity Implementatie Richtlijn Objecten RWS. In versie 1.0 van de Cybersecurity Implementatie Richtlijn Objecten waren al de nodige en beschikbare requirements uit de voorlopers van de IEC 62443 delen overgenomen en geïntegreerd. Om naar meer volledigheid en integratie van de recente IEC 62443 requirements te werken is samengewerkt met de Subject Matter Expert (SME) ten aanzien van de IEC 62443 om te toetsen welke requirements nog toegevoegd moest worden ten behoeve van de integratie voor versie 2.0 van de Cybersecurity Implementatierichtlijn Objecten.



De Subject Matter Expert heeft aangegeven welke requirements uit de relevante delen van de IEC 62443 ontbraken in versie 1.0 van de Cybersecurity Implementatie Richtlijn Objecten RWS en dus voor verrijking in aanmerking kwamen inclusief een advies wat de logische plaats was voor integratie. Vervolgens heeft dezelfde Subject Matter Expert geholpen met de daadwerkelijke integratie van de ontbrekende requirements uit de IEC 62443 in versie 2.0 van de Cybersecurity Implementatierichtlijn Objecten (CSIR). Vervolgens zijn de CSIR maatregelen en achterliggende uitwerkingen weer verankerd en geïntegreerd met de relevante BIO controls binnen de structuur van de NEN-ISO-27001 bijlage A.



De BIO is een baseline en de hieruit voor Industriële Automatisering relevante en afgeleide basisset aan controls moet dan ook worden gezien als de baseline controlset voor Industriële Automatisering **die altijd van toepassing is.** Voor een overzicht van de proces- en systeemtechnische baseline controlset wordt verwezen naar de vraagspecificatie/contract. Deze uit de BIO afgeleide baseline controlset voor IA zal echter niet alle kwetsbaarden en risico's afvangen die zich voordoen binnen de Industriële Automatisering. De kwetsbaarheden en risico's binnen de Industriële Automatisering zijn van een andere aard en orde en vragen om andere en aanvullende controls en maatregelen zoals ook opgenomen in de IEC 62443. De uit de BIO afgeleide basisset aan controls dienen uitgebreid te worden met aanvullende controls binnen de structuur van de NEN-ISO-27001 bijlage A die meer specifiek zijn voor de beveiliging van IA en een minimale plus set met verdiepende maatregelen in relatie tot de baseline IA controls. De minimale plus set aan verdiepende maatregelen in relatie tot de baseline IA controls dient dan ook minstens van het Security Level 1 te zijn zoals voorgeschreven vanuit de IEC 62443. De **Baseline beveiliging IA** (groene vlak in volgende afbeelding) kan dan ook langs deze weg gedefinieerd worden als de samenvoeging van de baseline beveiliging IA controls die een plus set aan verdiepende maatregelen aanroept die behoort bij het cybersecurity weerstandsniveau 1 zoals beschreven in hoofdstuk 2 van de Cybersecurity Implementatierichtlijn Objecten. De maatregelen die behoren bij cybersecurity weerstandsniveau 1 komen grotendeels overeen met de maatregelen die worden voorgeschreven vanuit de IEC 62443 voor het security level 1.



Om te kunnen bepalen of de Baseline beveiliging IA toereikend is of dat er nog meer aanvullende maatregelen moeten worden getroffen bovenop de baseline beveiliging IA dient altijd een risicoanalyse en afweging gemaakt te worden voor het definiëren van de plus set aan maatregelen boven op de baseline beveiliging IA. Om uitgebreide en complexe risicoanalyses te voorkomen voor het bepalen of de Baseline beveiliging IA maatregelen toereikend zijn of dat er nog meer aanvullende maatregelen nodig zijn, kunnen objecten op een pragmatische manier geclassificeerd worden naar de (ondersteunende) functies die ze vervullen in relatie tot het vitale primaire proces of Infrastructuur van de betreffende organisatie. Hiervoor dient een gangbare Business Impact Analyse (BIA) uitgevoerd te worden.

Bij het classificeren wordt pragmatisch gekeken naar de impact bij het uitvallen van de functie die het object vervult in relatie tot het primaire vitale proces van de organisatie en niet naar de oorzaken van uitval. Aan elke functiebox is een cybersecurity weerstandsniveau gekoppeld. Cybersecurity weerstandsniveau wordt hierbij gedefinieerd als het vermogen om weerstand te bieden tegen aanvallen die bedoeld zijn om zich met geweld of manipulatie toegang fysiek dan wel digitaal te verschaffen tot ruimten en of Industriële Automatiseringssystemen. De maatregelen uit de cybersecurity weerstandsniveaus corresponderen met de maatregelen voor de verschillende security levels zoals beschreven in de IEC 62443. In de functiebox indeling is Box A de hoogste functiebox indeling. Hoe hoger de functiebox indeling hoe weerbaarder een object voor cyberaanvallen moet zijn en dus meer maatregelen nodig zijn.

Toepasselijkheid CSIR

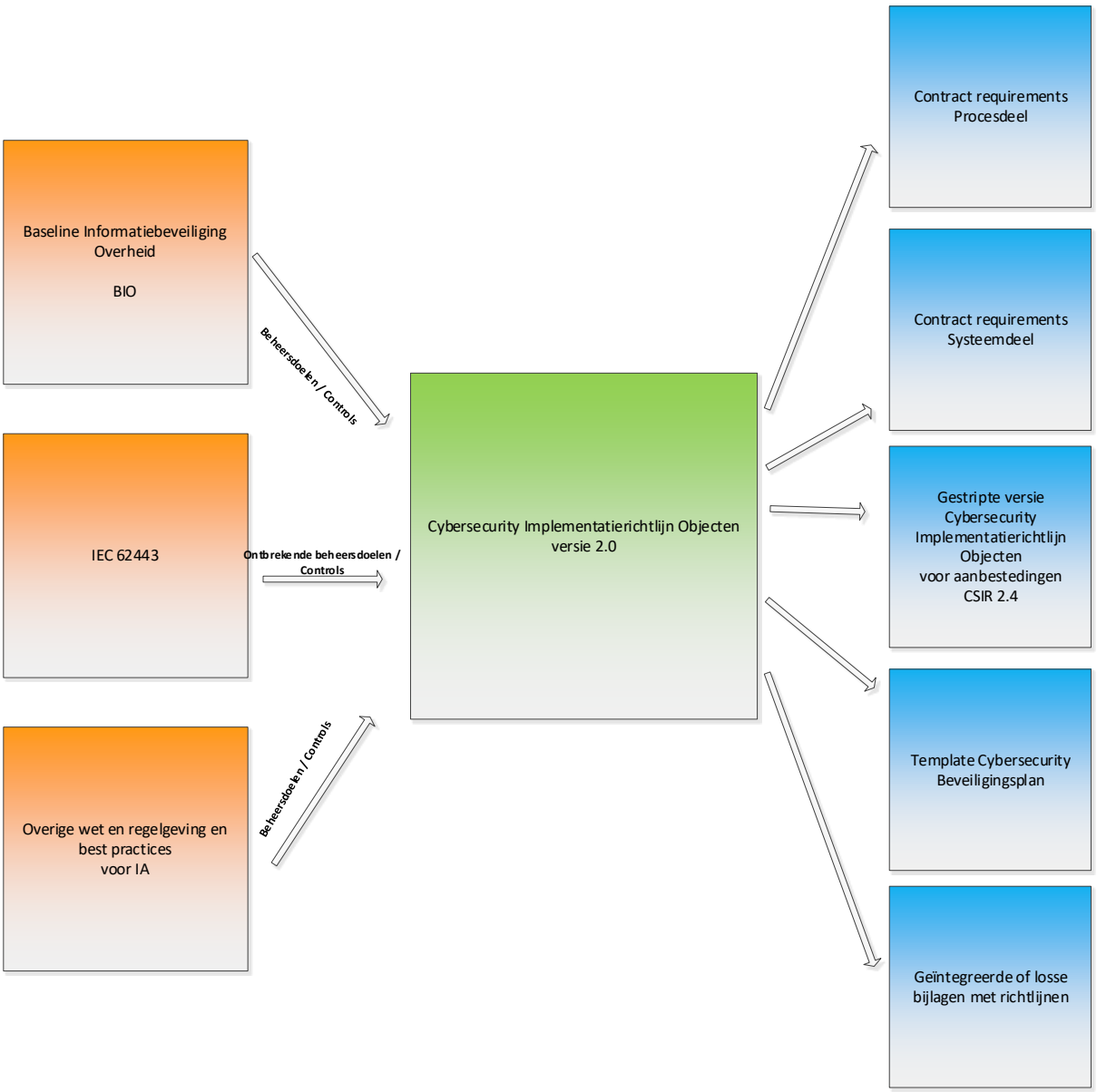
Elk beheerobject moet **minimaal uitgevoerd** worden met de Baseline beveiliging IA controls en de verdiepende aanvullingen (de plus maatregelen) uit hoofdstuk 2 waarbij cybersecurity weerstandsniveau 1 aangehouden moet worden. De richtlijnen in de bijlagen van de CSIR die ook vanuit de controls uit de vraagspecificatie/contract worden aangeroepen maken tevens onderdeel uit van de Baseline Beveiliging IA. De **Baseline beveiliging IA** is eigenlijk niet meer dan een bundeling en opstapeling van de controls en maatregelen uit de vraagspecificatie/contract die verdiepende uitwerkingen aanroepen uit hoofdstuk 2 van de CSIR waarbij het aangegeven cybersecurity weerstandsniveau aangehouden moet worden en de aangeroepen richtlijnen in de bijlagen van de CSIR.

De door de controls aangeroepen verdiepende uitwerkingen uit hoofdstuk 2 van de CSIR zijn maatregel pakketten om de meest voorkomende kwetsbaarheden en risico’s binnen de Industriële Automatiseringsomgeving te mitigeren. Bij de keuze voor deze verdiepende set van maatregelen is gebruik gemaakt van internationale onderzoeken naar de meest voorkomende kwetsbaarheden en risico’s binnen de Industriële Automatiseringsomgeving en de resultaten van interne onderzoeken. De door de controls aangeroepen verdiepende maatregelen pakketten staan ook in relatie tot de maatregelen van de security levels uit de IEC 62443. De toets door de Subject Matter Expert van de IEC 62443 heeft aangetoond dat de 10 paragrafen uit hoofdstuk 2 van de Cybersecurity Implementatierichtlijn Objecten samen met de controls uit de vraagspecificatie/contract en de richtlijnen in de bijlagen van de CSIR vergelijkbaar zijn met de security requirements uit de IEC 62443 voor de beveiliging van Industriële Automatisering.

Voor het bepalen van de verdiepende set van plus maatregelen uit hoofdstuk 2 is de functiebox indeling van het object nodig waaraan het cybersecurity weerstandsniveau is gekoppeld. Als het object geen functiebox indeling kent omdat er sprake is van losse IA componenten of oplossingen in het veld, dient altijd het cybersecurity weerstandsniveau 1 aangehouden te worden voor de verdiepende plus set aan maatregel uitwerkingen uit hoofdstuk 2 van de CSIR. De maatregelen moeten altijd in relatie staan tot de scope, toepassing en de risico’s hierbinnen. Afwijkingen op de

controls en maatregel implementatie dienen op basis van een risicoanalyse en afweging conform de uitgangspunten zoals die ook voor de BIO controls en maatregelen gelden verantwoord en via de explain procedure van de opdrachtgever behandeld te worden. In bijlage C is een best practice opgenomen voor het kunnen maken van risico afwegingen bij (tijdelijke) afwijkingen op de Baseline beveiliging IA controls en maatregelen.

Gebruik CSIR bij aanbestedingen
In geval van aanbestedingen wordt <u>een gestripte versie</u> van de RWS interne versie van de CSIR meegegeven bij aanbestedingen. De controls zoals opgenomen in de RWS interne versie van de CSIR worden vertaald naar proces en systeemtechnische eisen en opgenomen in de vraagspecificatie en of contract. Uit de RWS interne versie van de CSIR wordt het hoofdstuk met proces- en systeemtechnische controls verwijderd waardoor de gestripte versie CSIR 2.4 ontstaat voor aanbestedingen. De verschillende paragrafen uit hoofdstuk 2 en bijlagen van de CSIR 2.4 worden dan vanuit de vraagspecificatie of contract eisen aangeroepen. Zie de schematische weergave hieronder..



1.3 Instructie voor praktische toepassing

Gestreefd moet worden 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 functiebox indeling toegekend. De functiebox indeling correspondeert met een zgn. cybersecurity-weerstandsniveau, conform onderstaande tabel.

Classificatie object in functiebox

Functiebox indeling	Cybersecurity weerstandsniveau
A	4
B	3
C	2
D	1
E	

Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3. In dit document worden in de 10 paragrafen van hoofdstuk 2 de maatregelen beschreven per cybersecurity 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 object nog niet voorzien is van een cyber-classificatie dient er contact gezocht te worden met de beheerder/eigenaar van het object voor het (alsnog) classificeren en indelen van het object in een functiebox.

In het geval dat er helemaal geen sprake is van een echt object in de zin van een civiel technisch werk dan dient voor de beveiliging van de ICT en Industriële Automatisering en datanetwerkcomponenten binnen de eigen infrastructuur het cybersecurity weerstandniveau van 1 te worden aangehouden. Voorbeelden zijn pompkelders of kast ruimten in het areaal met ICT en IA componenten hierbinnen.

Ook kan het voorkomen dat de volledige set van de controls niet altijd van toepassing zijn omdat gewoonweg de risico’s zich niet in de scope van de overeengekomen opdracht voordoen. In dat geval dient men risico gestuurd te werken. De opdrachtgever maakt een selectie van de relevante controls en geeft dat in de vraagspecificatie mee. De opdrachtnemer dient altijd uit te gaan van de vraagspecificatie (controls) die bepaalde delen uit hoofdstuk 2 met verdiepingen en overige bijlagen met richtlijnen uit de Cybersecurity Implementatierichtlijn Objecten aanroept waarbij minimaal de maatregelen behorende bij cybersecurity weerstandsniveau 1 aangehouden moet worden voor de invulling. De bijlagen met richtlijnen moeten worden gezien als een best practice uitwerking en hierbinnen is geen onderscheid naar cybersecurity weerstandsniveau.

1.4 Inhoud

Hoofdstuk 1 bevat een inleiding, afleiding en toelichting op de werking van de Cybersecurity Implementatie Richtlijn Objecten.

Hoofstuk 2 met de 10 paragrafen bevat voor elk cybersecurity weerstandsniveau de verdiepende set met maatregelen voor de baseline beveiliging IA controls die onder andere uit de BIO zijn afgeleid. In de maatregelen set van hoofdstuk 2 van de CSIR zijn ook de maatregelen en of requirements uit de IEC 62443 delen als aanvulling en verdieping van de baseline beveiliging IA controls opgenomen. De tien paragrafen met de geclusterde thema's zijn afgeleid uit internationale onderzoeken naar de meest voorkomende kwetsbaarheden en risico's binnen de Industriële Automatiseringsomgeving en in relatie tot de maatregelen voor de security levels zoals voorgeschreven in de IEC 62443. De toets door de Subject Matter Expert met de IEC 62443 heeft aangetoond dat deze 10 paragrafen en thema's van de Cybersecurity Implementatierichtlijn Objecten dekkend zijn voor de IEC 62443 reguirements samen met de ruime uit de BIO afgeleide en vertaalde controls en ondersteunende richtlijnen in de bijlagen van de Cybersecurity Implementatierichtlijn Objecten die aangeroepen worden door de proces of systeem eisen zoals opgenomen in de vraagspecificatie of het contract voor de beveiliging van Industriële Automatisering. Opgemerkt moet worden dat de controls in de vraagspecificatie of contract ruimer kunnen zijn dan de controls die uit de BIO volgen en ook kunnen komen uit andere bronnen die meer specifiek zijn voor de beveiliging van vitale Infrastructuur en processen.

De bijlagen bevatten een aantal verdiepende richtlijnen en of templates/sjablonen waar gevraagde uitwerkingen in moeten worden vastgelegd en onderhouden. Met de templates/sjablonen wordt uniformering en uitwisselbaarheid van de cybersecurity maatregel uitwerking voor de objecten nagestreefd. Dit draagt bij aan uniforme beoordeling en sturing door object (risico) eigenaar, beoordelingen vanuit toezichthouders en de uitwisselbaarheid van cybersecurity uitwerkingen bij overgang van beheer en onderhoud werkzaamheden door andere marktpartijen.

2 Verdiepende maatregelpakketten

In de volgende paragrafen volgen de 10 aanvullende en verdiepende maatregelpakketten voor de controls die naar thema geclusterd zijn en gerelateerd aan de meest voorkomende kwetsbaarheden en risico's uit onder andere internationale onderzoeken binnen het werkveld van de Industriële Automatisering. De proces- en systeemtechnische controls uit de vraagspecificatie/contract roepen verschillende paragrafen uit hoofdstuk 2 van de CSIR aan. De opdrachtgever dient altijd de aan te houden proces- en systeemtechnische controls aan te geven die gevolgd moeten worden bij de uitvoering van het werk. Naast proces- en systeemtechnische controls uit de vraagspecificatie/contract dient ook het cybersecurity weerstandsniveau meegegeven te worden voor de beheerobjecten. Hierbij kan gebruikt gemaakt worden van de volgende vertaaltabel om te bepalen welk cybersecurity weerstandsniveau van toepassing is bij de functieboxen.

Object classificatie in functiebox	**Cybersecurity weerstandsniveau**
A	4
B	3
C	2
D	1
E	1

2.1 Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten

VRKI-referentie No.	Vereiste	Weerstandsniveau 1	2	3	4
F1	VRKI-referentie: 1	X			
F2	VRKI-referentie: 2		X		
F3	VRKI-referentie: 3			X	
F4	VRKI-referentie: 4				X

Toegangsbeheer No.	Vereiste	Weerstandsniveau 1	2	3	4
F5	Sleutel: Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)	X			
F6	Sleutel: Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)		X		
F7	Rijkspas kantoor: Toegang middels Rijkspas Kantoor installatienormen			X	X

Toegangsproces No.	Vereiste	Weerstandsniveau 1	2	3	4
F8	Lokaal geldende regels en processen zijn van toepassing.	X	X	X	X

Organisatorisch No.	Vereiste	Weerstandsniveau 1	2	3	4
F9	O1: Standaard organisatorische maatregelen.	X	X		
F10	O2: Als O1 met daarbij een omschrijving van de specifieke organisatorische maatregelen die zijn toegespitst op het risico-object.			X	X

Bouwkundig No.	Vereiste	Weerstandsniveau 1	2	3	4
F11	BK2: Bouwkundige maatregelen met prestatie-eis van 3 minuten inbraakwerendheid.	X	X		
F12	BK3: Bouwkundige maatregelen met prestatie-eis van 5 minuten inbraakwerendheid.			X	
F13	BK4: Bouwkundige maatregelen met prestatie-eis van 10 minuten inbraakwerendheid.				X

Compartimentering No.	Vereiste	Weerstandsniveau 1	2	3	4
F14	CO2: Compartimentering met prestatie-eis van 3 minuten inbraakwerendheid.	X	X		
F15	CO3: Compartimentering met prestatie-eis van 5 minuten inbraakwerendheid.			X	
F16	CO4: Compartimentering met prestatie-eis van 10 minuten inbraakwerendheid.				X
F17	ME2: Meeneem beperkende maatregel met prestatie-eis van 3 minuten diefstalvertraging.	X	X		
F18	ME3: Meeneem beperkende maatregel met prestatie-eis van 5 minuten diefstalvertraging.			X	
F19	ME4: Meeneem beperkende maatregel met prestatie-eis van 10 minuten diefstalvertraging.				X

Elektronische maatregelen No.	Vereiste	Weerstandsniveau 1	2	3	4
F20	EL2: Grade 2	X	X		
F21	EL3: Grade 2 / Grade 3			X	
F22	EL4: Grade 3 + maatwerk				X

F23	SD1: De schildetectie bestaat uit openstand detectie op nooduitgangen.	X	X		
F24	SD2: Schildetectie bestaat uit detectie, met als doel inbraaksignalering bij de eerste aanval op vaste en beweegbare gevelelementen van of voor, de periferie van ruimten waar de attractieve goederen zich bevinden.			X	
F25	SD3: Schildetectie als bij SD2 met als aanvulling dat (bereikbare) wanden, vloeren en daken zijn voorzien van geschikte detectie.				X

Alarmtransmissie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F26	AT2: ATS: SP2/DP1; security grade: 2; ontvangst PAC: T2	X	X		
F27	AT3: ATS: DP3; security grade: 3; ontvangst PAC: T4			X	
F28	AT4: ATS: DP4; security grade 3; ontvangst PAC: T5				X

Reactie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
F29	RE1: In deze situatie kan de alarmering door het inbraaksignaleringssysteem gemeld worden naar een (mobiele) telefoon (spraak, tekstbericht) die bereikbaar is. Bij bedrijven is dit een eis. De alarmopvolging kan geschieden door persoonlijke verificatie door de eigenaar of sleutelhouder(s).	X			
F30	RE2: Reactie alarmopvolging: alarmopvolging door sleutelhouder(s) die door de PAC worden gebeld. Bij de PAC moeten minimaal 3 sleutelhouders zijn opgegeven.		X		
F31	RE3: Reactie alarmopvolging: procedure als bij RE2 met de aanvulling dat voor de alarmopvolging een contract moet zijn gesloten met een door het Ministerie van Justitie en Veiligheid toegelaten particuliere beveiligingsorganisatie (geregistreerd middels ND nummer), die onder meer als sleutelhouder kan fungeren. Bij RE3 kan ook worden gekozen voor RE2 + technische alarmverificatie waarmee in plaats van alarmopvolging door een particuliere beveiligingsorganisatie alarmopvolging door een sleutelhouder samen met prioriteit 1 door de politie kan worden bereikt.			X	
F32	RE4: Reactie alarmopvolging: procedure als bij RE3 (dus opvolging door een particuliere beveiligingsorganisatie). Uitgangspunt is opvolgingstijd van maximaal 15 minuten door de particuliere beveiligingsorganisatie en een prioriteit 1 van de politie (15 minuten, na technisch alarmverificatie).				X

N.B.:

1. De in deze paragraaf beschreven fysieke beveiligingsmaatregelen hebben als scope de beveiliging van IA-gerelateerde ruimten. Hieronder wordt verstaan de bedienruimte en technische ruimten binnen de objectpanden. Voor de fysieke beveiliging van het complex/terrein en de hierbinnen gepositioneerde objectpanden dienen de maatregelen aangehouden te worden die volgen uit het locatiebeveiligingsplan. De fysieke beveiligingsmaatregelen uit het locatiebeveiligingsplan omvatten de samenvoeging en dus de opstapeling en integratie van de set van fysieke beveiligingsmaatregelen die volgen uit het Handboek Security RWS en de Cybersecurity Implementatierichtlijn Objecten. Bij constatering van overlap in de samenbundeling en integratie van maatregelen in het locatiebeveiligingsplan wordt de regel aangehouden dat de zwaarste maatregel uit één van de kaders wordt overgenomen. De fysieke beveiligingsmaatregelen uit het locatiebeveiligingsplan dienen vervolgens door het RWS projectteam vertaald te worden naar proces en systeemtechnische vereisten en integraal onderdeel uitmaken van de vraagspecificaties bij aanbestedingen.
2. Gemotiveerd afwijken van de hier genoemde maatregelen kan, bijv. als dat efficiënter is in de integrale aanpak vanuit het locatiebeveiligingsplan, als maar wel aan de bovenliggende weerstandseisen wordt voldaan door de stapeling en integratie van de set van fysieke beveiligingsmaatregelen in het locatiebeveiligingsplan.
3. Bij voorgaande maatregelen m.b.t. de fysieke toegangsbeveiliging van de IA-gerelateerde ruimten is aansluiting gezocht bij VRKI 2020.

2.2 Maatregelen logische toegang

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
LM11	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
LP1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.	X	X	X	X
LP2	Er dient erop toe te worden gezien dat: a. de toegang voor de bedienaars en beheerders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend plaatsvindt, rol gebaseerd en op basis van het 'need to have' en 'segregation of duties' principe; b. de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het strikt noodzakelijke; c. fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend wordt toegestaan voor personen die hiertoe geautoriseerd zijn; d. disciplinaire maatregelen worden genomen bij misbruik van accounts en autorisaties.	X	X	X	X
LP3	Er dient erop toe te worden gezien dat: a. de toewijzing en het gebruik van privileges van software en apparatuur beperkt dienen te blijven tot het noodzakelijke, zodat alleen geauthentiseerde apparatuur toegang kan krijgen tot een vertrouwde zone; b. het voor een geautoriseerde gebruiker mogelijk is om privileges te koppelen aan rollen voor alle menselijke gebruikers; c. gebruikersaccounts door een procuratiehouder tijdelijk kunnen worden opgeschort.	X	X	X	X
LP4	De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dienen minimaal eenmaal per halfjaar te worden beoordeeld en geactualiseerd in een formeel proces. Opvolging van de bevindingen is gedocumenteerd en wordt behandeld als een beveiligingsincident.	X	X	X	X
LP5	De lokale logische toegang voor medewerkers (op basis van functieprofiel) tot de RWS infrastructuur, ICT, ICS/SCADA systemen en de centrale en lokale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager te worden aangevraagd en goedgekeurd. Hierbij dient ten minste het volgende te worden gedocumenteerd: details van de accounthouder,	X	X	X	X

	autoriserend manager, permissies behorende bij het account, geautoriseerde apparatuur.				
LP6	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik te worden gemaakt van de diensten die RWS hiervoor beschikbaar stelt.	X	X	X	X
LP7	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	X	X	X	X
LP8	Beheerders, bedienaars en overig ondersteunend personeel wordt ondersteund in het beheren van hun wachtwoorden en krijgen hiertoe de beschikking over een wachtwoordkluis.	X	X	X	X
LP9	Toepassingen, functionaliteit of apparatuur om de toegangseisen te passeren mogen niet worden gebruikt.	X	X	X	X
LP10	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 dienen ook de voorgeschreven handelingen bij verlies, diefstal dan wel beschadiging te worden opgenomen.	X	X	X	X
LP11	Accounts dienen op uniforme wijze te worden beheerd.	X	X	X	X
LP12	De toegang voor beheer en onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van het beheer en onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en afgesloten bij afmelding van het onderhoud, dan wel automatisch beëindigd na de vooraf ingestelde periode van openstelling.	X	X	X	X
LP13	Systeemhulpmiddelen waarmee beheersmaatregelen kunnen worden omzeild dienen nauwkeurig te worden gecontroleerd en geminimaliseerd, waarbij uitsluitend bevoegd personeel toegang heeft tot deze hulpmiddelen en gebruik wordt gelogd en bewaard voor tenminste 6 maanden.	X	X	X	X
LP14	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Uitsluitend mag hiervan worden afgeweken na een expliciete risicoafweging op dit punt.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
LT1	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.	X	X	X	X

LT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.	X	X	X	X
LT3	Voor bedienaars, beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.	X	X	X	X
LT4	Voor bedienaars, beheerders, software processen en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon, software proces of systeem.			X	X
LT5	Het aantal gelijktijdige sessies dat kan worden opgezet door enige gebruiker (mens, software-proces of apparaat) dient te worden beperkt en instelbaar te zijn.	X	X	X	X
LT6	Toegang tot de programmabroncode behoort te worden beperkt.	X	X	X	X
LT7	(Standaard) wachtwoorden moeten door gebruikers bij het in gebruik nemen van de systemen gewijzigd kunnen worden .	X	X	X	X
LT8	Wanneer systemen alleen met generieke accounts kunnen werken, moet dit worden gemotiveerd, vastgelegd en de risico's in beeld gebracht en voorgelegd worden aan Opdrachtgever voor acceptatie van de afwijking om met generieke accounts te mogen werken.	X	X	X	X
LT9	Gedurende het gehele authenticatieproces dient er geen feedback te worden geven over de authenticatie-informatie.	X	X	X	X
LT10	Alvorens aan te melden dient een systeemnotificatie op het scherm te worden weergegeven. Hierin worden restricties omtrent (on)geautoriseerd systeemgebruik aangegeven, evenals logging en monitoring van het systeemgebruik.	X	X	X	X
LT11	Broncode van ontwikkelde programma's dient te worden beschermd en toegang tot de code beperkt.	X	X	X	X
LT12	De logische toegang dient als volgt te worden ingevuld: a. Lokaal bediening – minimaal een user-ID en wachtwoord combinatie; b. Lokaal beheer en administrator accounts – 'two-factor' authenticatie ('bezit' plus 'kennis'); c. Remote toegang voor beheer en onderhoud - 'two-factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.	X	X		
LT13	De logische toegang dient als volgt te worden ingevuld: a. Lokaal bediening, beheer en administrator accounts – Rijkspas Kantoor/vergelijkbaar elektronisch toegangsbeheersysteem ('bezit' plus 'kennis'); b. Remote toegang voor beheer en onderhoud - 'two-factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS/CIV. c. Apparatuur en applicaties dienen bij onderlinge task-to-task communicatie uniek geauthentiseerd te worden middels Mac-adres, en/of IP-adres, device naam, elektronische sleutel, etc.			X	X

LT14	Het gebruik van sterke wachtwoorden dient mogelijk te zijn en net als de vervangingsfrequentie te worden afgedwongen.	X	X	X	X
LT15	Indien 10 keer achter elkaar een foutieve inlogpoging plaatsvindt, dient het account voor een minimale periode van 24 uur te worden geblokkeerd.	X	X	X	X
LT16	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	X	X	X	X

2.3 Maatregelen beveiligingsincidenten en incident response plan

Mens		Weerstandsniveau			
No.	Vereiste	1	2	3	4
IM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
IP1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van externe partijen) beveiligingsincidenten 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) wordt geëist dat zij alle beveiligingsincidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.	X	X	X	X
IP2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.	X	X	X	X
IP3	Er 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 het incident. Bepaald wordt welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moeten worden gecommuniceerd naar en worden besproken met de bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van externe partijen).	X	X	X	X
IP4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op dat van RWS-CIV.	X	X	X	X
IP5	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via	X	X	X	X

	publieke netwerken zoals internet) wordt de Incident Manager van RWS-CIV ingeschakeld.				
IP6	Er dient een operationeel incident response plan te bestaan voor reactie op en afhandeling van incidenten en calamiteiten.	X	X	X	X
IP7	Er dient een operationeel recovery plan te bestaan voor recovery na incidenten of calamiteiten.	X	X	X	X
IP8	Jaarlijks dienen de incident response en recovery te worden beproefd aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van de jaarlijkse oefening is het testen van de noodbediening.	X	X	X	X
IP9	Tijdens een calamiteit kan het noodzakelijk zijn om het object te evacueren of deuren die toegang bieden tot IA-systemen, te openen voor hulpdiensten. Hierdoor hebben ook kwaadwillenden op dat moment toegang tot de IA-systemen. De bescherming van de vitale delen van het IA-systeem dient gedurende calamiteiten te zijn geborgd middels een procedure.			X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
IT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen te worden geactiveerd en benut voor registratie en rapportage van beveiligingsincidenten.	X	X	X	X
IT2	Indien het control systeem niet meer normaal kan functioneren als gevolg van een aanval, dient het control system naar een vooraf gedefinieerde veilige situatie te schakelen (bijvoorbeeld: unpowered, hold of fixed).	X	X	X	X
IT3	Het ICS/SCADA systeem dient na onderbreking of falen terug te kunnen keren naar een bekende veilige staat.	X	X	X	X
IT4	Het ICS/SCADA systeem en de bediening dienen te kunnen schakelen naar en van een noodstroomvoorziening zonder dat dit invloed heeft op de beveiligingsstatus van het object.	X	X	X	X
IT5	In geval van een DOS-aanval dient het ICS/SCADA systeem in een beperkte modus te kunnen functioneren om ten minste de toegang tot de safety systemen te waarborgen.			X	X

2.4 Maatregelen netwerkkoppelingen en cryptografie

2.4.1 Netwerkkoppelingen

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
NM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
NP1	Opdrachtnemer draagt zorg voor en ziet erop toe dat alle datanetwerkverbindingen van het lokale objectnetwerk met het RWS netwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten conform de "Nieuwe Netwerkvoorzieningen Verkeer en Waterstaat - Aansluitvoorwaarden" van Rijkswaterstaat (zal na gunning op verzoek van de Opdrachtnemer beschikbaar worden gesteld). Rechtstreekse (vaste of draadloze) toegang tot het Systeem vanuit andere netwerken dan die van RWS, of vice versa, is strikt verboden.	X	X	X	X
NP2	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.	X	X	X	X
NP3	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met RWS-CIV voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de RWS Netwerkarchitectuur inclusief security.	X	X	X	X
NP4	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 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. Streef naar maximale beveiliging en continue monitoring van deze netwerkkoppelingen.	X	X	X	X
NP5	Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke	X	X	X	X

	netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen kwetsbaarheden).				
NP6	Bij afname van netwerkdiensten via providers, of in het geval van samenwerkingsverbanden, dient geëist te worden dat maximale hardening is doorgevoerd op de ingezette netwerk componenten en of apparatuur.	X	X	X	X
NP7	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient uitsluitend plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.	X	X	X	X
NP8	Gestreefd moet worden naar maximale inzichtelijkheid van de datanetwerkkoppelingen van de objecten. Alle datanetwerkkoppelingen dienen in kaart te worden gebracht, zodat altijd duidelijk is via welk datanetwerkpad een actor (uiteindelijk) een object zou kunnen binnendringen, beginnend vanuit het internet.	X	X	X	X
NP9	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectdatanetwerken door middel van een Configuration Management Database (CMDB).	X	X	X	X
NP10	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt op en opvolging geeft aan geregistreerde datanetwerk incidentmeldingen vanuit RWS-CIV.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
NT1	ICS/SCADA en safety systemen, de ondersteunende systemen en besloten lokale objectnetwerken mogen alleen verbindingen hebben met kantoornetwerken indien deze verlopen via de beveiligde centrale voorzieningen van RWS.	X	X	X	X
NT2	Communicatie en functies van safety systemen zijn afgeschermd van overige communicatie.	X	X	X	X
NT3	De gebruikte communicatiemethoden dienen de integriteit van de gegevensoverdracht te borgen, inclusief fysieke en omgevingsinvloeden op de integriteit van de gegevensoverdracht.	X	X	X	X
NT4	De klokken van alle relevante informatie verwerkende systemen binnen een object behoren te worden gesynchroniseerd met één hiertoe aangewezen **centrale** referentietijdbron binnen het netwerk van Opdrachtgever.	X	X	X	X
NT5	Een back-up voor de referentietijdbron **lokaal** dient te zijn ingericht, opdat tijdsynchronisatie kan plaatsvinden in geval dat de centrale referentietijdbron van Opdrachtgever niet beschikbaar is.	X	X	X	X

2.4.2 *Cryptografie*

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
CM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
CP1	De Opdrachtnemer dient bij gebruik van cryptografie uitsluitend PKI-Overheid certificaten in te zetten voor communicatie met (externe) netwerken buiten de RWS infrastructuur. Deze kunnen via Opdrachtgever worden aangevraagd.	X	X	X	X
CP2	De Opdrachtnemer dient bij gebruik van cryptografie uitsluitend PKI-RWS certificaten in te zetten voor communicatie binnen de interne RWS infrastructuur. Deze kunnen via Opdrachtgever worden aangevraagd.	X	X	X	X
CP3	De Opdrachtnemer heeft ten minste de volgende onderwerpen uitgewerkt in het cryptografiebeleid: a. Wanneer wordt cryptografie ingezet; b. Wie is verantwoordelijk voor de implementatie; c. Wie is verantwoordelijk voor het sleutelbeheer; d. Welke normen dienen als basis voor cryptografie en de op welke wijze worden de normen van het Forum Standaardisatie toegepast; e. Op welke wijze wordt het beschermingsniveau vastgesteld; f. Welke procedures gevolg worden voor de communicatie tussen organisaties onderling; g. Het gebruik, bescherming en levensduur van de cryptografische sleutels.	X	X	X	X
CP4	De Opdrachtnemer kiest bij gebruik van cryptografie voor cryptografische toepassingen die voldoen aan passende standaarden en heeft dit gedocumenteerd.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
CT1	Bij inzet van versleuteling (cryptografie) dient de gekozen versleuteling en de onderliggende algoritmes en instellingen uitsluitend de duiding "goed" te hebben zoals aangegeven in de meest actuele versie van het NCSC document "Richtlijnen voor Transport Layer Security".	X	X	X	X
CT2	Indien het configureren van de IA/PA/OT systemen op afstand plaatsvindt, dan dient dit over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door de Opdrachtgever het	X	X	X	X

	onveilige communicatieprotocol worden ingezet, mits er een additioneel versleuteld kanaal wordt toegepast (SSL, TLS, IPSEC etc.). De gekozen versleuteling en de onderliggende algoritmes en instellingen dienen dan uitsluitend de duiding "goed" te hebben zoals aangegeven in de meest actuele versie van het NCSC document "Richtlijnen voor Transport Layer Security".				

2.5 Maatregelen bescherming tegen kwetsbaarheden

2.5.1 Anti-malware

Mens		Weerstandsniveau			
No.	Vereiste	1	2	3	4
AM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
AP1	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware.	X	X	X	X
AP2	Bij 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.			X	X
AP3	Opdrachtnemer dient te beschikken over een recoveryplan, waarin zijn opgenomen: alle nodige voorzieningen voor back-up en herstel, kopieën van gegevens en programmatuur, evenals benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware.	X	X	X	X
AP4	Voor zover technisch te scannen dienen zowel intern ontworpen, als ingekochte systemen en applicaties, jaarlijks te worden gescand op fouten in code, malware en generieke beveiligingskwetsbaarheden.			X	X
AP5	Opdrachtnemer draagt er aantoonbaar zorg voor (en ziet er op toe) dat gegevensdragers, beheer- en onderhoudsapparatuur gecontroleerd is op en vrij is van malware voordat deze worden gekoppeld aan ICS/SCADA of overige ICT-systemen en lokale objectdatanetwerken.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
AT1	Antimalware voorzieningen moeten worden ingezet in overeenstemming met RWS-CIV, waarbij de opdrachtnemer, beheerder dient aan te kunnen tonen dat de antimalware software correct is geïnstalleerd en geconfigureerd. De juiste werking dient hierbij te kunnen worden aangetoond.	X	X	X	X
AT2	Antimalware voorzieningen moeten worden ingezet in afstemming met RWS-CIV voor de in- en uitgangen tot de systeemzones. Zoals removable media, firewalls, unidirectional gateways, web servers, proxy servers en remote-access servers.			X	X
AT3	Updates van de signatures, anti-malwaresoftware en bijbehorende herstelsoftware dienen dagelijks plaats te vinden.	X	X	X	X
AT4	De anti-malware voorzieningen mogen geen invloed hebben op de werking en functionaliteit van in gebruik zijnde ICS/SCADA en ICT-systemen.	X	X	X	X

2.5.2 *Hardening*

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
HM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
HP1	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen.	X	X	X	X
HP2	Hardware, software en netwerkapparatuur dienen op basis van een analyse veilig geconfigureerd te worden waarbij gebruik wordt gemaakt “good practice security baselines”.	X	X	X	X
HP3	Opdrachtnemer dient aan te tonen welke hardening-methoden zijn gebruikt en hoe deze zijn toegepast.	X	X	X	X
HP4	Het weer inschakelen van uitgezette services en/of protocollen mag alleen door geautoriseerd personeel worden uitgevoerd.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
HT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig te worden (her)geconfigureerd dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet is toegestaan. Ook dient het gebruik van mobiele code beperkt te worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij: a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd.	X	X		
HT2	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. Ook dient het gebruik van mobiele code beperkt te worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij: a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd; c. het gebruik van mobiele code wordt gemonitord; d. voor gebruik een integriteitscheck op de mobiele code wordt uitgevoerd.			X	X
HT3	Gedeeld geheugen (b.v. RAM) dient te worden leeggemaakt voordat het gedeeld geheugen wordt vrijgegeven voor andere gebruikers.			X	X
HT4	Minimale hardening maatregelen zijn: a. niet noodzakelijke datanetwerkservices uit te zetten; b. het verwijderen (patchen) van bekende kwetsbaarheden; c. alle poorten die niet nodig zijn te deactiveren/blokkeren; d. alle default "access points" te verwijderen; e. de default accounts uit te schakelen conform het wachtwoord policy; f. indien beschikbaar gebruik te maken van de security opties van leveranciers.	X	X	X	X
HT5	Het weer functioneel kunnen aanzetten van uitgeschakelde services en/of protocollen moet mogelijk blijven.	X	X	X	X

2.5.3 *Patching*

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
PM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
PP1	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. Patches mogen het niveau van systeem hardening niet aantasten.	X	X	X	X
PP2	Bij patches 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.	X	X	X	X
PP3	Indien patches om bepaalde redenen bewust niet worden uitgevoerd, dient de afweging hiertoe schriftelijk te worden vastgelegd voorzien van een risicoafweging, inclusief een mitigatievoorstel.	X	X	X	X
PP4	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.	X	X	X	X
PP5	Opdrachtnemer dient over een geborgde procedure voor patching te beschikken waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden en procuratiehouders.	X	X	X	X
PP6	Indien zowel de kans op misbruik als de verwachte schade hoog zijn (volgens de NCSC-classificatie voor kwetsbaarheidswaarschuwingen), wordt de betreffende patch in overleg met Opdrachtgever ingepland voor implementatie. In de tussentijd worden op basis van een expliciete risicoafweging tijdelijke mitigerende maatregelen getroffen.	X	X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
PT1	Het uitvoeren van securityfuncties (b.v. netwerkscans, patching) mag de beschikbare systeemresources niet zodanig beperken dat de normale softwareprocessen op de ICS/SCADA systemen hiervan zichtbaar hinder ondervinden.			X	X

2.6 Maatregelen logging en monitoring

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
MM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
MP1	Opdrachtnemer draagt zorg voor en ziet er op toe dat: a. de loggegevens worden weggeschreven en opgeslagen in een apart bestand, dat alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; b. de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen worden beschermd tegen verlies of wijziging; c. op basis van een expliciete risicoafweging de bewaarperiode van de logbestanden (van alle systemen met logvoorziening) wordt bepaald. Deze bewaartermijn is altijd tenminste drie maanden; d. loggegevens die zijn gebruikt voor incidentonderzoeken, langer worden bewaard conform de bewaartermijnen die de (feiten)onderzoekers aangeven; e. er een overzicht is van alle logbestanden die worden gegenereerd; f. een (onafhankelijke) interne audit procedure ten minste elke 6 maanden toetst op het ongewijzigd bestaan van de logbestanden g. het oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens, zo snel mogelijk wordt gemeld als beveiligingsincident via de procedure voor beveiligingsincidenten.	X	X	X	X
MP2	De RWS Objectverantwoordelijke/-beheerder dient expliciet toestemming te verlenen voor de levering van logbestanden aan derden.	X	X	X	X
MP3	Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het ICS/SCADA en de gekoppelde ICT-componenten in kaart gebracht. Een geborgde procedure is aanwezig om te bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.			X	X
MP4	Camerabeelden van verkeersregistratiesystemen dienen gelogd en gemonitord te worden.	X	X	X	X
MP5	De Opdrachtnemer dient zijn medewerking te verlenen voor het kunnen analyseren van het netwerkverkeer van en naar het object	X	X	X	X

	en binnen het lokale object netwerk door het Security Operations Centre (SOC) van Opdrachtgever.				
MP6	De Opdrachtnemer dient een analyse poort binnen de netwerkinfrastructuur van het object in te richten en beschikbaar te houden voor sensoren die door Opdrachtgever gekoppeld moeten kunnen worden aan deze analyse poort.	X	X	X	X
MP7	De Opdrachtnemer dient het ontwerp voor de inrichting van de analyse poort en de fysieke plaatsing van de sensor voor afstemming en acceptatie voor te leggen aan het RWS CIV IRN Netwerkteam/SOC van Opdrachtgever.	X	X	X	X
MP8	De opdrachtnemer dient voor de goede werking van de analyse poort (beheer-)documentatie op te stellen en te onderhouden.	X	X	X	X
MP9	De Opdrachtnemer dient indien het object niet permanent op het Security Operations Centre is aangesloten zijn medewerking te verlenen voor het incidenteel kunnen uitlezen van het lokale object netwerkverkeer of een specifiek deelnetwerk van het object middels de analyse poorten.	X	X	X	X
MP10	De Opdrachtnemer dient over een operationeel proces te beschikken als onderdeel van het incidentmanagementproces voor het melden van incidenten aan, en de response op meldingen van, het SOC van Opdrachtgever.	X	X	X	X
MP11	De Opdrachtnemer dient over een operationeel proces te beschikken voor de registratie en rapportage van netwerk storingen binnen het lokale objectnetwerk aan de Opdrachtgever.	X	X	X	X
MP12	De opdrachtnemer dient voor het ontwerp en inrichting van de analysepoort en de fysieke plaatsing van de sensor binnen (bestaande) lokale objectnetwerken gebruik te maken van de door Opdrachtgever voorgeschreven netwerkproducten en -diensten.	X	X	X	X
MP13	De Opdrachtnemer dient ontdekte nieuwe dreigingen te delen met Opdrachtgever.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
MT1	De handelingen van medewerkers, beheerders, operators, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in audit-logbestanden.	X	X	X	X
MT2	Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen te worden gedetecteerd, gerapporteerd en voorkomen.	X	X		
MT3	Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen automatisch te worden gedetecteerd, gerapporteerd en voorkomen.			X	X

MT4	Logregels bevatten minimaal de volgende gegevens: a. de gebeurtenis zelf; b. Benodigde informatie om de actie te kunnen herleiden tot een natuurlijk persoon, b.v. gebruikersnaam of een (systeem)-ID; c. component waarop de handeling werd uitgevoerd; d. het resultaat van de handeling; e. de datum en het tijdstip van de gebeurtenis; f. een doorlopende en unieke nummering per logregel.	X	X	X	X
MT5	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en ICT-netwerkelementen dienen in CSV-formaat opgeleverd te worden.	X	X	X	X
MT6	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.	X	X	X	X
MT7	Het overschrijven of verwijderen van logregels en logbestanden wordt gelogd in een nieuw aangelegde log.	X	X	X	X
MT8	De loginstellingen en logbestanden worden zodanig beschermd dat deze niet benaderd, gewijzigd of gewist kunnen worden door ongeautoriseerden.	X	X	X	X
MT9	Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen moeten beveiligingsspecifieke logsystemen worden ingezet, in afstemming met (en op verzoek van) Opdrachtgever.			X	X
MT10	Indien er fouten optreden tijdens het verwerken van de loggegevens, dient er een waarschuwing te worden gegeven.	X	X	X	X
MT11	Werking van de logging van security-gerelateerde events dient door Opdrachtnemer aantoonbaar te worden gemaakt door middel van een door RWS goedgekeurd gesimuleerd security-gerelateerd event.			X	X
MT12	De robuustheid van de logging (bij grote aantallen gelijktijdig optredende gebeurtenissen) dient te worden aangetoond en beschreven door Opdrachtnemer.			X	X
MT13	Er dient voldoende ruimte te zijn voor audit opslag (logging), en maatregelen zijn genomen die de kans beperken dat de beschikbare ruimte overschreden wordt. Er dient tijdig een waarschuwing te worden gegeven indien de opslagcapaciteit op dreigt te raken.			X	X
MT14	Het object datanetwerk dient uitgevoerd te zijn met analysepoorten waarbij datanetwerk ontwerp van het object met eventuele onderkende deeldatanetwerken leidend is voor het aantal in te richten analysepoorten op de datanetwerken. Eén poort op het datanetwerk dient dan geconfigureerd te zijn als analysepoort.	X	X	X	X
MT15	Het object datanetwerk dient uitgevoerd te zijn met een datanetwerk ontwerp en inrichting, zodanig dat een volledige kopie via de analysepoorten van al het bedien en besturingslaag	X	X	X	X

	netwerkverkeer (bijvoorbeeld de SCADA en PLC systemen) uitgelezen en opgebouwd kan worden, dat over het objectdatanetwerk met eventuele onderkende deeldatanetwerken gaat en kan worden aangeleverd voor analyse doeleinden.				
MT16	Het object dient zodanig uitgevoerd te zijn dat de sensor van Opdrachtgever fysiek geplaatst kan worden binnen het lokale datanetwerk en de hiertoe voorziene technische ruimte en of kast. Voor de specificaties van de sensor dient Opdrachtnemer contact en afstemming te zoeken met Opdrachtgever.	X	X	X	X
MT17	Het object dient zodanig ingericht en beschikbaar te zijn dat de permanente of incidentele analyse van het lokale datanetwerk verkeer of een specifiek deeldatanetwerk van het object door Opdrachtgever via de analyse poorten moet kunnen plaatsvinden.	X	X	X	X
MT18	De inrichting van de analyse poort en de fysieke plaatsing van de sensor binnen bestaande lokale objectdatanetwerken dient uitgevoerd te worden met de door Opdrachtgever voorgeschreven datanetwerkproducten en -diensten.	X	X	X	X
MT19	Alle relevante informatie-verwerkende systemen en de daarbij behorende logging systemen dienen te worden gesynchroniseerd met één referentietijdbron, waarvan de integriteit is gevalideerd.	X	X	X	X

2.7 Maatregelen bewustwording en training

2.7.1 Medewerkers

Medewerker No.	Vereiste	Weerstandsniveau 1	2	3	4
TMe1	Bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door het management aangegeven en beschikbaar gestelde periodieke Cybersecurity bewustwording en awareness cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen. De bewustwording en awareness trainingen besteden ook aandacht aan Sociaal Engineering.	X	X	X	X
TMe2	Iedere opdrachtnemer, bedienaar, beheerder en overig ondersteunend personeel 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.	X	X	X	X
TMe3	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.	X	X	X	X
TMe4	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.	X	X	X	X
TMe5	Bij het constateren van een security incident dienen 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: a. Uitval van diensten, apparatuur of voorzieningen, systeemstoringen of overbelasting als gevolg van cybersecurity inbreuken; b. menselijke fouten die leiden tot functionele verstoring of uitval van systemen; c. inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; d. hack pogingen via de infrastructuur van opdrachtnemer en/of zijn netwerkproviders tot het netwerkdomein van opdrachtgever; e. inbreuk op de bediening en beheer; f. ongeautoriseerde systeemwijzingen; g. niet-naleving van beleid of gedragsregels; h. detectie van malware bij ad hoc controles/scans; i. virusmeldingen vanuit operationele antimalwarevoorzieningen; j. verlies of diefstal van ICT en IA bedrijfsmiddelen; k. oneigenlijk gebruik van bevoegdheden;	X	X	X	X

	l. vandalisme, moedwillige beschadiging.				
TMe6	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.	X	X	X	X
TMe7	Opdrachtnemer, Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden of onveilige situaties als gevolg van cybersecurity inbreuken, die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen, dan wel de schade beperken.	X	X	X	X
TMe8	Bedienaars, beheerders en overig ondersteunend personeel 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.	X	X	X	X
TMe9	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.	X	X	X	X
TMe10	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de regels in acht voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen.	X	X	X	X
TMe11	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA omgeving, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd hiervan zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.	X	X	X	X
TMe12	Voor 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.	X	X	X	X
TMe13	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.	X	X	X	X
TMe14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en toegekende autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen of werken. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.	X	X	X	X

TMe15	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT-systemen en netwerken de standaard/default/fabrieks-accounts en/of wachtwoorden bij ingebruikname te verwijderen, uit te schakelen of ten minste te wijzigen.	X	X	X	X
TMe16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.	X	X	X	X
TMe17	Alleen geautoriseerde medewerkers/beheerders mogen systemen koppelen aan objectdatanetwerken of ICS/SCADA systemen. Deze systemen dienen voorzien te zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen	X	X	X	X
TMe18	Gegevensdragers worden altijd vooraf op malware gecontroleerd, voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.	X	X	X	X
TMe19	Mobiele apparatuur mag niet onbeheerd achtergelaten worden in openbare, vergader-, en conferentieruimten, in auto’s of andere vervoermiddelen.	X	X	X	X
TMe20	Verlies of diefstal van mobiele apparatuur dient spoedig mogelijk te worden gemeld als een security incident.	X	X	X	X
TMe21	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.	X	X	X	X
TMe22	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.	X	X	X	X
Tme23	Beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur wordt gelockt, ondersteund door een automatische lock na een vooraf in te stellen periode van inactiviteit.	X	X	X	X
TMe24	Opdrachtnemers, bedienaars, beheerders en overig personeel zijn zich bewust van de wijze waarop zij met vertrouwelijke informatie om te dienen te gaan, van het aanmaken en gebruiken van informatie tot vernietiging ervan.	X	X	X	X
TMe25	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.	X	X	X	X
TMe26	Medewerkers mogen zonder voorafgaande goedkeuring geen apparatuur, informatie of software van de locatie meenemen.	X	X	X	X

TMe27	Het is voor gebruikers niet toegestaan zelf software te installeren.	X	X	X	X

2.7.2 *Managers*

Manager No.	Vereiste	Weerstandsniveau 1	2	3	4
TMa1	Er dient bewerkstelligd te worden dat een ieder continu (dus ook bij aanstelling en functiewisseling) bewust wordt gemaakt door Opdrachtnemer en (valideerbaar) geschikte training, regelmatige bijscholing krijgt (en ook begrijpt) en geïnformeerd wordt met betrekking tot het (cybersecurity) beveiligingsbeleid, procedures, en verantwoordelijkheden ten aanzien van cyber security, voor zover relevant voor hun functie. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk. Een ieder die zich bezig houdt met risicomanagement dient hier kennis van te hebben, dan wel hiervoor specifieke aanvullende training te ontvangen.	X	X	X	X
TMa2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: a. aantoonbaar kennis hebben van cybersecurity; b. de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is. Daarbij dient bijgehouden te worden wanneer aanvullende training wenselijk dan wel noodzakelijk is; c. de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; d. 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; e. ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; f. dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als 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; g. 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. Opdrachtnemer dient veranderingen van personeel of subcontractors die toegang hebben tot de besturingssystemen van objecten ook direct kenbaar te maken aan opdrachtgever; h. dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten;	X	X	X	X

	i. gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.				
TMa3	De Opdrachtnemer/objectverantwoordelijke/-beheerder/verantwoordelijk management bespreken en evalueren 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 kunnen worden vermeden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen. Feedback van medewerkers dient actief te worden opgevolgd teneinde cybersecurity te verbeteren.		X	X	X
TMa4	Opdrachtnemer ziet erop toe (en heeft contractueel vastgelegd)_dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging, zoals fysieke en logische toegang, melding van beveiligingsincidenten en gebruik van bedrijfsmiddelen. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steekproefsgewijze controles vastgesteld en uitgevoerd.			X	X
TMa5	Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.	X	X	X	X
TMa6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg altijd het betreffende account en wachtwoord te laten wijzigen.	X	X	X	X

2.8 Maatregelen gecontroleerd wijzigen

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
WM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
WP1	Opdrachtnemer beschikt over een geborgde procedure voor het (laten) inventariseren en registreren van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB). Deze CMDB dient actueel te worden gehouden.	X	X	X	X
WP2	Opdrachtnemer beschikt over een geborgde wijzigingsprocedure voor het doorvoeren van wijzigingen aan ICS/SCADA, ondersteunende ICT-systemen, beveiligings- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.	X	X	X	X
WP3	Wijzigingen mogen alleen worden aangevraagd en uitgevoerd door geautoriseerden.	X	X	X	X
WP4	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 zijn goedgekeurd door de Objectverantwoordelijke/-beheerder voordat uitvoering van werkzaamheden plaatsvindt.			X	X
WP5	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 situatie en afwijkingen in de CMDB worden gecorrigeerd.	X	X	X	X
WP6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten vooraf aan de implementatie in productie worden getest in een testomgeving (inclusief verslaglegging) om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit van het systeem of de beveiliging van de organisatie. Afwijken hiervan is uitsluitend mogelijk indien Opdrachtgever hiervoor toestemming geeft en dit schriftelijk wordt vastgelegd. Testen in de productieomgeving mag uitsluitend na voorafgaande goedkeuring door Opdrachtgever en na vastlegging hiervan. Alle testgegevens dienen zorgvuldig te worden gecontroleerd en beschermd.			X	X
WP7	Gegevensdragers en updates van software en firmware van technische systemen dienen eerst gescand te worden op malware	X	X	X	X

	voordat zij aan ICT of IA systemen worden gekoppeld en/of geïnstalleerd.				
WP8	De authenticiteit/integriteit van de software voor ICS/SCADA en overige ondersteunende ICT-systemen moet worden gecontroleerd voorafgaand aan de implementatie op operationele systemen.			X	X
WP9	Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn doorgevoerd als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.	X	X	X	X
WP10	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. Direct 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.			X	X
WP11	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.	X	X	X	X
WP12	Er wordt gebruik gemaakt van testvoorzieningen, om de door te voeren wijzigingen en/of security patches vooraf te testen.	X	X	X	X

Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
WT1	Ontwikkel-, test-, acceptatie, productie en Leeromgeving (OTAPL) behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen door minimaal de volgende maatregelen: a. Functionele scheiding van de ontwikkel, test, acceptatie, productie en leeromgeving; b. De omgevingen zijn qua systemen en netwerk logisch of fysiek van elkaar gescheiden; c. Gebruikers dienen voor elke omgeving met andere gebruikersprofielen te kunnen werken; d. Voor de gebruikers is het helder in welke omgeving er wordt gewerkt; e. Elke omgeving dient conform de logrichtlijnen handelingen in logfiles vast te leggen die alleen toegankelijk is voor geautoriseerden; f. Er is een geborgd proces voor versiebeheer van de OTAPL.	X	X	X	X
WT2	Indien leverbaar dient het ICS/SCADA systeem en bijbehorende ICT-systemen de mogelijkheid te ondersteunen om de geïnstalleerde componenten en hun kenmerken te kunnen rapporteren.	X	X	X	X

2.9 Maatregelen beheer en onderhoud

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
OM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
OP1	Opdrachtnemer draagt zorg voor het evalueren van risico's en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cycle management.	X	X	X	X
OP2	Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers: a. geheimhouding is opgenomen; b. training- en opleidingsvereisten alsmede overige benodigde certificeringen zijn beschreven; c. screening van personeel is geregeld (bijv. VOG); d. beschreven is dat de beveiligingshuisregels van Opdrachtgever strikt in acht moeten worden genomen; e. een concrete procedure is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) en dat deze bij alle betrokkenen bekend is; f. de procedures voor fysieke toegang tot objecten en ruimten, alsook de logische toegang tot systemen zijn vastgelegd; g. de registratie en rapportage van beveiligingsincidenten is geregeld; h. beschreven is dat handelingen van medewerkers en systemen worden gelogd en gemonitord ; i. de procedure "Toegang Derden" van de CIV voor de logische toegang tot netwerken en systemen moet worden gevolgd. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. j. beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die zijn voorzien van de laatste security updates, patches en actuele viruscontroleprogrammatuur; k. beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van RWS verlopen; l. beschreven is dat wijzigingen conform het wijzigingsproces van RWS mogen worden uitgevoerd; m. beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden van RWS moeten worden uitgevoerd; n. beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; o. beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het RWS- of objectnetwerken strikt verboden is.	X	X	X	X
OP4	Opdrachtnemer draagt zorg voor de beschikbaarheid, onderhoud en accuraat houden van (technische) beheerdocumentatie	X	X	X	X

	(waaronder fysieke en logische netwerktekeningen, verbindingen en configuratie documenten en een inventaris van alle apparatuur en software, inclusief versie- en serienummers), 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.				
OP5	Opdrachtnemer draagt zorg voor een geborgde procedure die de personele toegang van al het vaste onderhoudspersoneel regelt voorafgaand aan de uitvoering van werkzaamheden.			X	X
OP6	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: a. het doorvoeren van wijzigingen conform de wijzigingen procedure; b. de procedure voor fysieke toegang; c. de procedure voor logische toegang; d. patching, back-up procedure en bewaartermijnen; e. incidentmanagement, log- en incidentrapportages en de analyse daarvan.	X	X	X	X
OP7	Opdrachtnemer dient jaarlijks de opzet, het bestaan en de werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever en het Cybersecurity Beveiligingsplan bijgewerkt en voorgelegd te worden aan de Opdrachtgever.		X	X	X
OP8	RWS Bedrijfsvertrouwelijk is alleen op basis van het 'need-to-know' principe toegankelijk voor de medewerkers van Rijkswaterstaat en de Opdrachtnemer.	X	X	X	X
OP9	Rijkswaterstaat en 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.	X	X	X	X
OP10	Geprinte exemplaren van documenten met classificatie RWS Bedrijfsinformatie dienen in afgesloten kasten bewaard te worden. Bij digitale opslag in de eigen kantooromgeving is versleuteling niet verplicht.	X	X	X	X
OP11	Opdrachtnemer dient zowel actieve als passieve apparaten te controleren op malware voordat deze worden verbonden met, of gebruikt in, de IA-omgeving.	X	X	X	X
OP12	Het koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen bij een object, dient op veilige wijze te gebeuren.	X	X	X	X
OP13	Apparatuur dient correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen	X	X	X	X

Techniek		Weerstandsniveau			
		1	2	3	4
OT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend (RWS en extern) personeel tot objecten en	X	X	X	X

	de ruimten hierbinnen, wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.				
OT2	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.	X	X	X	X
OT3	Gedurende FAT, SAT en onderhoud dient de werking van de cybersecurityfuncties in de systemen te kunnen worden aangetoond.	X	X	X	X
OT4	Gedurende FAT, SAT en onderhoud dient de werking van de cybersecurityfuncties in de systemen geautomatiseerd te kunnen worden aangetoond middels tooling.			X	X
OT5	Het koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen bij een object, dient op veilige wijze te gebeuren.	X	X	X	X

2.10 Maatregelen back-ups

Mens No.	Vereiste	Weerstandsniveau 1	2	3	4
BM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel (zowel van RWS als die van Opdrachtnemer) wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie No.	Vereiste	Weerstandsniveau 1	2	3	4
BP1	Systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging. Wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd. Met deze back-up moet men in staat zijn middels een volledige roll-back naar de werkende situatie terug te kunnen gaan. Indien back-ups gedurende de operationele fase van een object gemaakt moeten worden, dan mag dit het operationele proces niet verstoren.	X	X	X	X
BP2	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: a. 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 bevindt; b. 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; c. Back-ups worden bewaard tot het moment van uitdienstname van het betreffend systeem; d. In geval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.	X	X	X	X
BP3	Opdrachtnemer heeft gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.	X	X	X	X
BP4	Opdrachtnemer controleert en test jaarlijks de herstelprocedures 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.		X	X	X
BP5	Opdrachtnemer evalueert maandelijks de gemelde incidenten en storingsmeldingen inzake back-up en treft waar nodig maatregelen.		X	X	X

Techniek No.	Vereiste	Weerstandsniveau 1	2	3	4
BT1	Opdrachtnemer richt in overleg met Opdrachtgever de benodigde voorzieningen in voor het back-up en restoreproces.	X	X	X	X

Bijlage CSR 1 Omgaan met vertrouwelijke informatie en documenten

CSR 1.1 Doelstelling

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 cybercriminaliteit. 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. De classificatie geeft de aard van de documentatie weer en helpt de gebruiker bij het bepalen hoe een document verwerkt dient te worden.

Rijkswaterstaat houdt de volgende rubricering of informatieclassificatie aan:

a. Departementaal Vertrouwelijk;
b. RWS Bedrijfsvertrouwelijk;
c. RWS Bedrijfsinformatie.

Departementaal Vertrouwelijk

Deze informatie dient strikt vertrouwelijk te worden behandeld en mag uitsluitend op basis van need-to-know worden verstrekt. Informatie met deze classificatie mag niet worden uitgewisseld met Opdrachtnemers en valt derhalve buiten de scope van dit document.

RWS Bedrijfsvertrouwelijk

Deze informatie is uitsluitend toegankelijk voor diegenen die de informatie nodig hebben om hun werkzaamheden uit te kunnen voeren en wordt op basis van need-to-know verstrekt.

RWS Bedrijfsinformatie

Deze informatie is voor iedereen vrij toegankelijk.

CSR 1.2 Best practice

CSR 1.2.1 Uitwisselen van informatie

In de overeenkomst tussen Rijkswaterstaat en een Opdrachtnemer zijn eisen opgenomen voor geheimhouding en het vertrouwelijk omgaan met documenten.

Voorbeelden van RWS bedrijfsvertrouwelijke informatie (gerelateerd aan cybersecurity) zijn:

a. Ontwerpdocumenten, constructietekeningen en -berekeningen;
b. Bediening en beheer handleidingen, veiligheidsinstructies en documentatie;
c. Configuratiedocumentatie van ICT en ICS/SCADA-systemen;
d. Datanetwerkschema’s en IP adressen;
e. Informatie over de ligging van kabels en leidingen;
f. Informatie over accounts en wachtwoorden.

Uitwisseling van informatie kan op meerdere manieren plaatsvinden. Voor elke wijze van uitwisseling zijn specifieke voorwaarden en regels van kracht:

Informatie uitwisseling via email

a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer.
b. Informatie met de classificatie TLP AMBER mag onversleuteld via email worden uitgewisseld tussen Rijkswaterstaat en BAW partners.

Informatie uitwisseling via bestand-uitwisselingsservices

a. Informatie met de classificatie RWS Bedrijfsvertrouwelijk via Wetransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en Opdrachtnemer, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de

wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

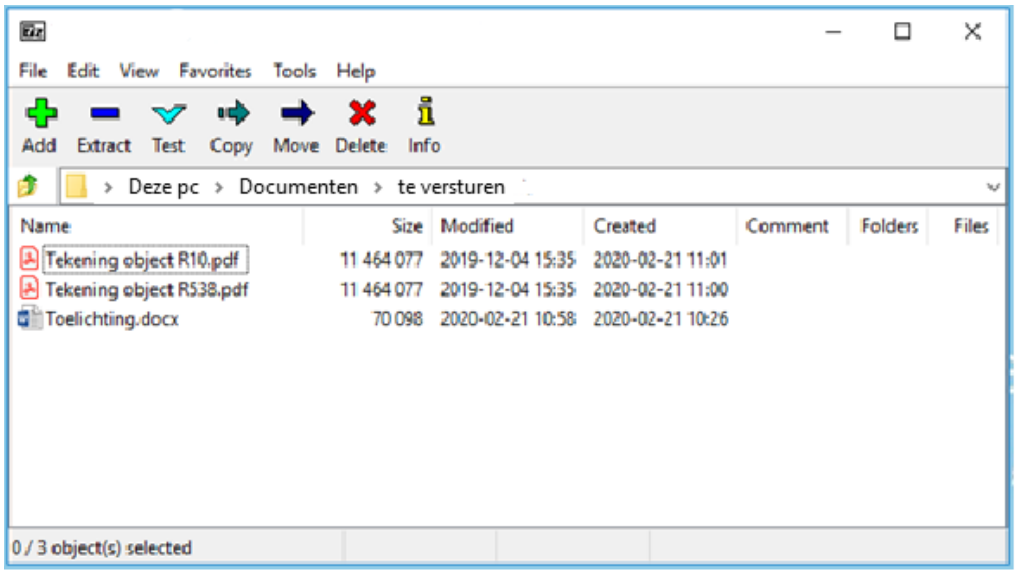
b. Informatie met de classificatie TLP AMBER via Wetransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld tussen Rijkswaterstaat en BAW partners, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

Informatie uitwisseling via servers van opdrachtnemer of opdrachtgever
Informatie met de classificatie RWS Bedrijfsvertrouwelijk of TLP AMBER mag onversleuteld via servers van opdrachtgever, opdrachtnemer of BAW partner worden uitgewisseld, mits er een voldoende authenticatie van de gebruiker en zijn bevoegdheden plaatsvindt.

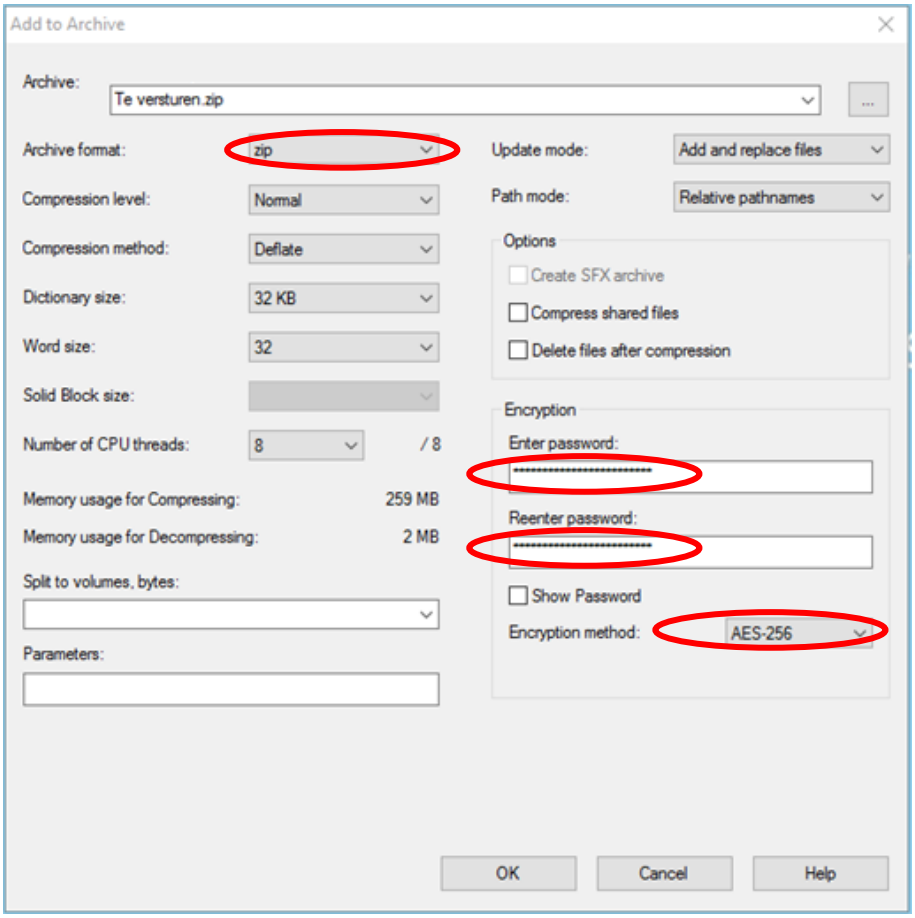
CSR 1.2.2 Versleutelen van gegevens
Wanneer versleuteling van informatie nodig is, dient dit te gebeuren met ten minste AES 256 encryptie en een sterk wachtwoord dat voldoet aan de vereisten voor wachtwoorden. Voor versleuteling maakt RWS gebruik van 7-Zip. Dit is een eenvoudig te gebruiken computerprogramma, waarmee bestanden versleuteld ingepakt kunnen worden.
7-Zip is standaard aanwezig op de RWS werkplek en is tevens gratis voor (thuis)gebruik (zie www.7-zip.org). Bij gebruik van AES-256 versleuteling en sterke wachtwoorden (zie hiervoor de wachtwoordrichtlijn) biedt 7-Zip een veilige manier voor gegevensversleuteling.

Documenten versleutelen met 7-Zip

a. Start 7-Zip via de Start toets links onderin Windows.
b. Ga naar de folder waar de te versleutelen bestanden staan.



c. Selecteer de bestanden en klik op de Add button (het groene + symbool).



d. Selecteer:
   i. Archive format: zip
   ii. Encryption method: AES-256
e. Kies een wachtwoord dat voldoet aan de wachtwoordrichtlijn en voer dit in.
f. Klik op de OK button en sluit 7-Zip af.
g. Het versleutelde bestand is klaar om te versturen.

Documenten ontsleutelen met 7-Zip

a. Open het bestand in 7-zip.
b. Selecteer de Extract button (het blauwe − symbool).
c. Selecteer de folder waar het bestand uitgepakt dient te worden.
d. Voer het wachtwoord in en klik de OK button.

CSR 1.2.3 Overdracht en vernietiging van vertrouwelijke data bij einde contract

Bij het aflopen en beëindiging van een contract draagt de Opdrachtnemer alle voor het onderhoud (en onderhoudshistorie) relevante objectinformatie -met de classificatie Bedrijfsvertrouwelijk- gestructureerd over aan Rijkswaterstaat.
Daarna vernietigt Opdrachtnemer de overgebleven Bedrijfsvertrouwelijke informatie en verwijdert deze alle Bedrijfsvertrouwelijke informatie van de eigen systemen.

Bijlage CSR 2 Personele toegang

CSR 2.1 Doelstelling

Het van belang inzicht te hebben in wie toegang heeft tot de IA systemen binnen de objecten. Van onderhoudspersoneel dient te worden vastgesteld dat verwacht kan worden dat zij op juiste wijze zullen omgaan met informatie waartoe men toegang heeft.

CSR 2.2 Best practice

Best practices voor personele toegang zijn als volgt (indachtig naleving van AVG regels):

a. De Opdrachtnemer dient te verzorgen dat al het vast onderhoudspersoneel voorafgaand aan zijn/haar operationele inzet:
   i. een persoonlijke geheimhoudingsverklaring heeft ondertekend;
   ii. zich daarbij kan legitimeren met een officieel geldig legitimatiemiddel met een goed gelijkende pasfoto;
   iii. een Verklaring Omtrent Gedrag (VOG) bezit welke is gerelateerd aan de beoogde Werkzaamheden;
b. 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:

a. Zich legitimeert;
b. 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.

Bijlage CSR 3 Architectuur objectnetwerk

CSR 3.1 Doelstelling

RWS streeft bij elk van de objecten naar een netwerkinfrastructuur die in lijn is met de te beschermen belangen en de geïdentificeerde risico's. Middels deze richtlijn wordt richting gegeven aan de cyberweerbaarheid van de objectnetwerken. Om de cyberweerbaarheid van de totale RWS ICT netwerk infrastructuur te waarborgen is het noodzakelijk dat elk te koppelen object dusdanig is ontworpen dat de cyberweerbaarheid gewaarborgd is. De hierbij gemaakte ontwerpkeuzes en bijbehorende maatregelen hebben als doel het object weerbaar te maken tegen cyberdreigingen, met een minimale impact bij een mogelijk cyberincident.

Het is van belang dat de gemaakte architectuurkeuzes van een objectnetwerk de gestelde maatregelen ondersteunen. Dat betreft enerzijds een veilige inrichting van het objectnetwerk zelf en anderzijds een zodanige inrichting dat data op een veilige en betrouwbare wijze ontsloten kan worden.

Deze richtlijn is bedoeld voor de medewerkers van de opdrachtnemer die tijdens nieuwbouw- of renovatieproject een netwerk voor het object specificeren en ontwerpen.

CSR 3.2 Best Practice

CSR 3.2.1 Inleiding

Binnen Rijkswaterstaat wordt onderscheid gemaakt in de netwerken voor de Informatie Voorziening (IV) en de netwerken voor de Industriële Automatisering (IA) ook wel Procesautomatisering (PA) of Operationele Technologie (TO) genoemd.
Binnen het IV netwerk wordt voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid gewerkt volgens het RWS zoneringsmodel. Dit RWS zoneringmodel voor het IV netwerk is gebaseerd op het zoneringsmodel van de NORA[2].

Echter voor objectnetwerken wordt deze segmentering op basis van vertrouwelijkheidsniveaus niet toegepast. In plaats daarvan wordt een zonering toegepast op basis van een risicobeoordeling van het object.

Voor de segmentering van het objectnetwerk geldt het uitgangspunt: "een apart netwerksegment voor elke onderkende functie voor het functioneren van het object".

Voor de verschillende netwerksegmenten geldt het volgende:

a. Netwerksegmenten zijn fysiek of logisch van elkaar, gescheiden (er kan geen verkeer vrij tussen verschillende segmenten worden uitgewisseld);
b. Voor de netwerksegmenten is bepaald aan welke zones deze gekoppeld kunnen zijn;
c. Netwerk toegang door gebruikers is rol gebaseerd en per zone onder controle.

In een verzameling netwerksegmenten over verschillende objecten geldt een restrictie voor het onderlinge verkeer. Een object mag niet direct verkeer uitwisselen met een object op een andere locatie. Dit mag alleen via een gecontroleerd en gemonitord koppelvlak. Er mag wel verkeer plaatsvinden tussen het object en de centrale bedienlocatie.

CSR 3.2.2 Risicobeoordeling

Om tot een juiste netwerksegmentatie te komen wordt van opdrachtnemer verwacht dat er op basis van een risico beoordeling een zoneringsmodel van het objectnetwerk wordt gemaakt. In het zoneringsmodel worden (op basis van een abstracte weergave) afgebakende netwerken met IV en IA voorzieningen weergegeven. Binnen een zone kunnen gegevens vrij worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken. Het doel van zonering is het isoleren van risico's zodat bedreigingen en incidenten uit de ene zone niet kunnen doorwerken in de andere zone.

[2] https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering

Op basis van een netwerkontwerp met netwerksegmentering wordt invulling gegeven aan het gedefinieerde zoneringsmodel.

Hiervoor dienen de volgende stappen te worden doorlopen:

a. Identificeer het totale systeem dat valt onder de opdracht;
b. Bepaal de cybersecurity risico's van het systeem en de deelsystemen;
c. Deel, op basis van de geïdentificeerde risico's, het systeem op in zones en de benodigde verbindingen tussen de zones;
d. Pas de maatregelen toe behorende bij het weerstandsniveau van het object;
e. Bepaal de overgebleven risico's voor elke zone;
f. Neem aanvullende cybersecurity maatregelen om de overgebleven risico's te mitigeren.

CSR 3.2.3 Uitgangspunten

Hierbij dienen de volgende uitgangspunten in acht te worden genomen:

a. Binnen een object worden op basis van de risico inventarisatie aparte netwerksegmenten ingericht.
b. Het zoneringsmodel dient te voldoen aan de maatregelen zoals vereist vanuit het weerstandsniveau van het object;
c. Het objectnetwerk bestaat uit een gelaagde opbouw die aansluit op het Purdue model;
d. Bedreigingen en incidenten uit de ene zone mogen niet doorwerken in de andere zone.
e. Zones kunnen logisch worden gescheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding;
f. Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak. Deze koppelvlakken staan uitsluitend het noodzakelijke netwerkverkeer toe;
g. Voor de geïdentificeerd noodzakelijke communicatie tussen segmenten moet een risico beoordeling worden gemaakt en de juiste maatregelen zijn getroffen om de geïdentificeerde risico's te mitigeren;
h. Waar mogelijk wordt gebruik gemaakt van de beschikbare RWS bouwblokken;
i. Als er vereisten zijn vanuit safety dan worden die meegenomen in het netwerkontwerp.

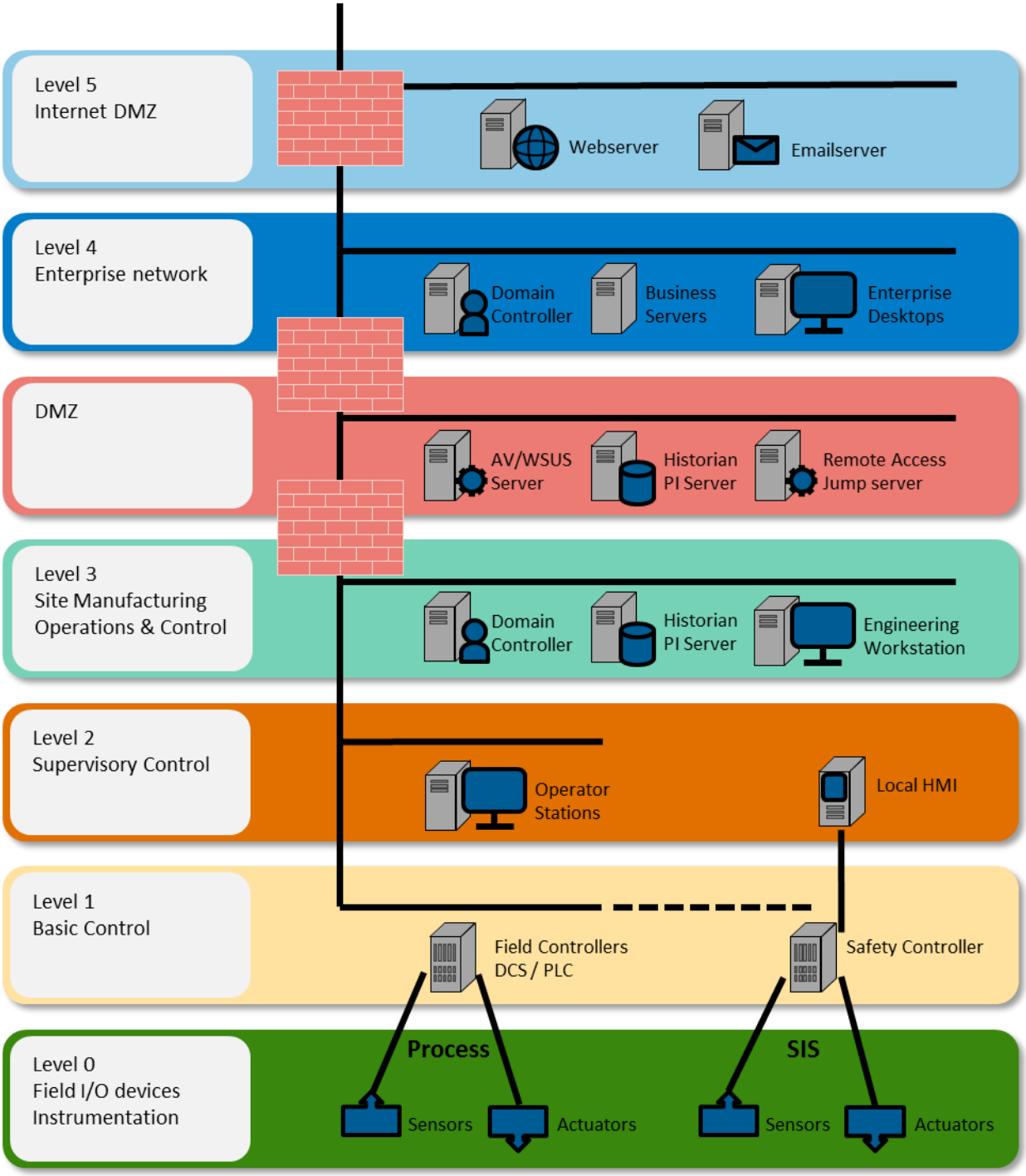
CSR 3.2.4 Gelaagde opbouw van het netwerk

In industriële omgevingen wordt voor de gelaagde opbouw van de netwerkinfrastructuur gerefereerd naar het Purdue model. Dit model gaat ervanuit dat er een aantal lagen zijn te onderscheiden, waarbij er tussen laag 3 en 4 een DMZ wordt ingericht om communicatie tussen IV en IA op digitaal veilige wijze te laten verlopen:

a. Laag 5 is de DMZ tussen het bedrijfsnetwerk en de externe netwerken;
b. Laag 4 is het bedrijfsnetwerk;
c. DMZ om IV en IA netwerken te scheiden (laag 3,5);
d. Laag 3 is gereserveerd voor Operations management;
e. Laag 2 bevat de lokale bediening;
f. Laag 1 bevat de veld controllers;
g. Laag 0 bevat de sensors en actuatoren, ofwel de interface tussen de elektronische wereld en de fysieke wereld.

CSR 3.2.5 Inrichting van het netwerk

Elke overgang tussen twee segmenten dient zodanig ingericht te zijn dat (in beide richtingen) geen verkeer wordt doorgelaten tenzij het noodzakelijk is ("deny by default") voor het veilig functioneren van het object. Daarnaast dient het objectnetwerk functioneel autonoom te zijn en derhalve zodanig te zijn ingericht en uitgerust dat het object ook op basis van lokale bediening kan functioneren. De werking van het object mag niet afhankelijk zijn van de beschikbaarheid van externe netwerken (island mode functie).



CSR 3.2.6 Koppelvlakken

Bijzondere aandacht dient besteed te worden aan de koppelvlakken tussen de verschillende segmenten. Daarbij zijn de volgende situaties te onderscheiden:

a. Koppelvlakken tussen segmenten binnen het object:
   De beveiliging van deze koppelvlakken wordt bepaald door een risicobeoordeling op de verschillende zones van het object.
b. Koppelvlakken met het DMZ:
   De beveiliging van deze koppelvlakken wordt bepaald door een risicobeoordeling met expliciet aandacht voor de koppeling met het DMZ en externe netwerken.

Bijlage CSR 4 Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen

CSR 4.1 Doelstelling

Tijdens het verrichten van beheer- onderhoudswerkzaamheden wordt door medewerkers van de Opdrachtnemer soms tijdelijk apparatuur (bijvoorbeeld draagbare media, waaronder USB-sticks, externe disks, laptop, tablet, CD's, DVD's, enz.)gekoppeld aan de ICT- en IA-omgeving (PLC's, servers, routers, switches, enz.) van Rijkswaterstaat. Hierdoor ontstaan cybersecurity risico's zoals b.v. malwarebesmetting of binnendringing van het netwerk. De Opdrachtnemer dient deze risico's te mitigeren.

CSR 4.2 Best practice

CSR 4.2.1 Soorten apparatuur

Met betrekking tot het koppelen van apparatuur wordt er onderscheid gemaakt tussen een tweetal soorten apparaten:

a. Actieve apparaten;
b. Passieve apparaten.

Actieve apparaten
Onder actieve apparaten wordt verstaan apparaten die zelfstandig kunnen opereren en over een Operating System beschikken, zoals b.v. een laptop of tablet.

Passieve apparaten
Onder passieve apparaten wordt verstaan apparaten die een actief apparaat nodig hebben voor informatie-uitwisseling. Dit zijn gegevensdragers en opslagmedia, zoals b.v. USB-sticks, externe disks, DVD's, CD-ROM's.

CSR 4.2.2 Instructies voor gebruik van actieve apparaten

Initieel

a. Zorg dat het apparaat gehardend is;
b. Versleutel de harde schijf van het apparaat;
c. Beveilig de toegang tot het apparaat met een sterk wachtwoord;
d. Installeer een malwarescanner;
e. Zet de interne firewall aan op het apparaat.

Vóór en tijdens elk gebruik

a. Gebruik het apparaat uitsluitend voor beheer en onderhoud van IA systemen van Rijkswaterstaat;
b. Alvorens verbinding te maken met het IA netwerk op de objecten, installeer de laatste updates en patches;
c. Alvorens verbinding te maken met het IA netwerk op de objecten, installeer de laatste updates van de malwarescanner en scan het apparaat;
d. Alvorens verbinding te maken met het IA netwerk op de objecten, download de benodigde updates en patches voor ICT en IA systemen;
e. Alvorens verbinding te maken met het IA netwerk op de objecten, download ICT of IA-software (updates en patches) uitsluitend vanaf een betrouwbare bron en via een beveiligde verbinding;
f. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de integriteit van downloads van ICT en IA software met de meegeleverde hashcode;
g. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de downloads op malware voordat deze worden geïnstalleerd binnen de ICT of IA omgeving;
h. Alvorens verbinding te maken met het IA netwerk op de objecten, zet 3G, 4G, 5G, WiFi, Bluetooth uit (koppelingen tussen IA en andere netwerken zijn niet toegestaan) en laat deze gedurende de koppeling met het IA netwerk uit staan;
i. Alvorens verbinding te maken met het IA netwerk op de objecten, dienen mobiele gegevensdragers door Opdrachtnemer ter controle gescand te worden op malware.

CSR 4.2.3 Instructies voor gebruik van passieve apparaten

Gebruik uitsluitend de voorgeschreven opslagmedia voor de koppeling met ICT- of IA-systemen;
Zorg dat alle gegevens op USB-sticks en externe harde schijven versleuteld zijn, volgens de richtlijn voor het omgaan met vertrouwelijke gegevens;
Scan gegevensdragers zoals b.v. USB-sticks, externe harde schijven, CD-ROM's, DVD's en diskettes elke keer vóór gebruik binnen de ICT- of IA-omgeving op malware;
Vervang een gegevensdrager waarop malware is ontdekt door een nieuwe gegevensdrager;
Alvorens verbinding te maken met het IA netwerk op de objecten, dienen gegevensdragers door Opdrachtnemer ter controle gescand te worden op malware.

CSR 4.2.4 Smartphones en Tablets

Smartphones en Tablets mogen niet worden ingezet voor bediening. Bij voorkeur ook niet voor beheer en onderhoudswerkzaamheden, aangezien deze niet kan voldoen aan de gestelde veiligheidseisen.

Bijlage CSR 5 Draadloze netwerken

CSR 5.1 Doelstelling

Middels draadloze communicatie is het mogelijk om op afstand te communiceren met een ander apparaat. WIFI, infrarood, Bluetooth, LoRa, 4G en 5G zijn enkele methoden voor draadloze communicatie. In tegenstelling tot bedrade communicatie hoeft een aanvaller geen fysieke toegang te hebben tot het netwerk of de apparatuur. Doelstelling is draadloze communicatie zo veel mogelijk te beperken en (waar gebruikt) te beveiligen tegen binnendringing en/of manipulatie.

CSR 5.2 Best practices

Basisuitgangspunt is dat de draadloze interfaces in apparaten en systemen zijn uitgeschakeld. Waar draadloze communicatie toch wordt ingezet, geldt het volgende:

a. Het gebruik van draadloze communicatie voor besturing en bediening van een object is niet toegestaan;
b. Het gebruik van draadloze communicatie voor het doorgeven van meetinformatie voor meten is uitsluitend toegestaan als het communicatiekanaal niet gebruikt kan worden voor configuratie, herstarten, uitschakelen of op enige andere wijze manipuleren van de meeteenheid;
c. Het gebruik van draadloze communicatie (o.a. WIFI, Bluetooth, IR, maar niet beperkt hiertoe) voor configuratie van apparatuur is uitsluitend toegestaan als de mogelijkheid tot draadloze communicatie na configuratie wordt uitgeschakeld;
d. Het draadloze netwerksegment is (bij voorkeur fysiek) gescheiden van het overige netwerk;
e. Communicatie tussen het draadloze netwerk en het vaste IA netwerk loopt via een beveiligd koppelvlak;
f. Bij draadloze verbindingen wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven;
g. Voor de inzet van draadloze communicatie dient een risicoanalyse en afweging gemaakt te worden waarin ook de restrisico’s en compenserende maatregelen zijn uitgewerkt;
h. Daar waar draadloze communicatie wordt toegepast dient dit te worden gedocumenteerd en onderhouden;
i. Telemetriesystemen o.b.v. GPRS, 4G, 5G enz. dienen koppelingen tussen SIM-kaart ID en Mac-adres van het bijbehorende apparaat vast te leggen;
j. De risicoanalyse en –afweging dient voorgelegd te worden aan het Security Centre van RWS/CIV voor goedkeuring;
k. Draag zorg voor passende fysieke beveiliging van de draadloze netwerkcomponenten om te voorkomen dat kwaadwillenden toegang hebben tot de infrastructuur;
l. Draadloze communicatie dient op een veilige wijze geconfigureerd te worden;
m. Draadloze communicatie dient te worden gelogd in overeenstemming met de logging richtlijn.

Bijlage CSR 6 IoT

CSR 6.1 Doelstelling

Internet of Things (IoT) apparatuur vindt ook binnen de IA steeds meer zijn weg. Het is van belang om deze apparatuur op een cyberveilige wijze te gebruiken.

CSR 6.2 Best practices

Voor gebruik van IoT apparatuur binnen de IA-omgeving dient tenminste te worden voldaan aan het volgende:

a. Voordat IoT wordt ingezet dient een risico en privacy assessment te zijn uitgevoerd en zijn waar relevant mitigerende maatregelen getroffen;
b. IoT toepassingen worden net als IA toepassingen beheerd en onderhouden en zijn derhalve opgenomen in het asset management CMDB, waarbij alle mogelijkheden om gegevens te verzamelen zijn gedocumenteerd;
c. IoT mag uitsluitend worden gebruikt voor het verzamelen van (meet)gegevens of telemetrie, niet voor het sturen of besturen van installaties;
d. IoT apparaten dienen in een apart netwerksegment te worden geplaatst dat is gescheiden middels een firewall die uitsluitend de noodzakelijke communicatie doorlaat;
e. Verschillende IoT systemen worden van elkaar geïsoleerd;
f. Principes van least privileges en hardening (uitschakelen debug interfaces, software services en andere niet gebruikte functionaliteit) worden toegepast;
g. Risico gestuurd dienen kwetsbaarhedenscans uitgevoerd te worden voor de gebruikte IoT apparatuur. Hierbij is aandacht voor kwetsbaarhedenscans, netwerk en penetratietesten;
h. IoT apparaten dienen gebruik te maken van wachtwoorden die voldoen aan de gestelde vereisten voor wachtwoord;
i. Elk IoT apparaat heeft een uniek, sterk wachtwoord dat niet af te leiden is uit andere wachtwoorden, device naam of gebruikersnaam. Hierbij dient de wachtwoordrichtlijn te worden gevolgd;
j. Pas waar mogelijk, en in overeenstemming met het weerstandsniveau van het object en de te beschermen functionaliteit, two-factor authenticatie toe;
k. Alle niet gebruikte protocollen dienen te worden uitgeschakeld;
l. Niet gebruikte (logische en fysieke) poorten dienen te worden uitgeschakeld of afgesloten;
m. IoT toepassingen worden risico gestuurd technisch gemonitord;
n. Foutieve inlogpogingen worden gelogd;
o. Het aantal foutieve inlogpogingen wordt beperkt;
p. IoT toepassingen worden voor ingebruikname afdoende getest.
q. IoT systemen vallen ook onder het regime van incident management, patchmanagement, configuratiemanagement en changemanagement;
r. De gebruikte IoT apparatuur dient voordat deze kan worden gebruikt, voldoende authenticatie te bieden, die in overeenstemming is met het weerstandsniveau van het object;
s. Security by design principes en secure development processes worden opgevolgd;
t. De life cycle van IoT apparatuur is vastgelegd en wordt nageleefd;
u. Vermijdt het gebruik van proprietary protocollen en versleutelingsalgoritmen, en pas uitsluitend bekende, gedocumenteerde en updatebare protocollen en versleutelingsalgoritmen toe;
v. IoT apparaten dienen te kunnen herstarten vanaf een vooraf gedefinieerde en beveiligde configuratie en daarbij de integriteit van de software te kunnen controleren;
w. Alle beschikbare beveiligingsmaatregelen op de IoT apparaten staan standaard aan;
x. Bij verwerking van persoonsgegevens dient te worden voldaan aan de AVG;
y. Inzet van IoT apparatuur dient zodanig te zijn ontworpen en geïmplementeerd dat grootschalige uitval ervan (door onbeschikbaarheid of compromittering) niet kan leiden tot uitval of onbeheersbaarheid van het object, of waardoor onacceptabele risico’s ontstaan;
z. IoT apparaten kunnen zelfstandig herstellen van tijdelijke uitval van netwerkfunctionaliteit en/of stroomuitval en hun functie hervatten;

aa. Het is op eenvoudige en gedocumenteerde wijze mogelijk om (vertrouwelijke of persoonlijke) informatie van het IoT apparaat te verwijderen;
bb. Secure setup en validatie daarvan is gedocumenteerd;
cc. Er is een Coordinated Vulnerability Disclosure (CVD) policy voor de IoT apparatuur;
dd. Alle security parameters dienen op een veilige en versleutelde wijze te worden opgeslagen op het apparaat.

Bijlage CSR 7 Wachtwoorden

CSR 7.1 Doelstelling

Wachtwoorden zijn een essentiële authenticatiemethode om personen, assets of processen toegang te geven tot die functionaliteit en gegevens die noodzakelijk zijn voor het uitvoeren van de beoogde functie, alsook om deze te beschermen tegen oneigenlijk gebruik door anderen. In deze richtlijn zijn de minimale best practices opgenomen, die binnen Rijkswaterstaat gelden voor het gebruik, wijzigen en beschermen van wachtwoorden in IA systemen.

Met de steeds verder toenemende rekenkracht van computers is het van belang dat wachtwoorden complex genoeg zijn en blijven, om weerbaar te blijven tegen tools om wachtwoorden te kraken. Het gebruik van sterke wachtwoorden met een voldoende complexiteit maakt het economisch onrendabel en praktisch onhaalbaar om wachtwoorden binnen de IA-omgeving van objecten te achterhalen.

Het is van groot belang dat Opdrachtnemers in lijn werken met de minimale vereisten voor wachtwoordcomplexiteit en ervoor zorgen dat de complexiteit van alle gebruikte wachtwoorden met de tijd meegaat.

CSR 7.2 Best practice

CSR 7.2.1 Vereisten aan wachtwoorden

Aan wachtwoorden voor alle gebruikers (zowel personen als processen) worden eisen gesteld m.b.t. lengte, complexiteit, geldigheidsduur en hergebruik:

a. Wachtwoorden hebben een minimale lengte, passend bij het soort account;
b. Wachtwoorden hebben een minimale complexiteit (verplichte karakterset) waaruit het wachtwoord moet bestaan:
    i. Hoofdletters;
    ii. Kleine letters;
    iii. Cijfers;
    iv. Speciale karakters, bijvoorbeeld: “;’:<>,.?!@#$%&*()+=_-^/\;
c. Wachtwoorden hebben een maximale geldigheidsduur;
d. Wachtwoorden kunnen niet worden hergebruikt.

Deze eisen zijn afhankelijk van het soort gebruikersaccount en gebruik. In algemeenheid geldt: hoe meer rechten aan een account zijn toegekend, hoe zwaarder de eisen.

De volgende zaken dienen niet te worden opgenomen in, of onderdeel uit te maken van, wachtwoorden:

a. Namen van familieleden, huisdieren, vrienden, collega’s, stripfiguren, etc.;
b. Computernamen en -termen, commando’s, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd;
c. Woorden verwijzend naar organisatie, object of locatie, bijvoorbeeld: Rijkswaterstaat, Amaliasluis, Rotterdam;
d. Geboortedata en andere persoonlijke informatie als adres en telefoonnummers;
e. Eén van de voorafgaande woordsoorten, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.).

CSR 7.2.2 Gegevensversleuteling

Voor versleuteling van gegevens t.b.v. gegevensuitwisseling dienen wachtwoorden te voldoen aan:

a. Wachtwoordlengte: minimaal 8 karakters;
b. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

CSR 7.2.3 Soorten accounts

Voor de IA-omgeving van objecten worden verschillende accounts onderkend, met elk hun eigen vereisten voor wachtwoordgebruik.

Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT- en IA-producten van fabrikanten mogen niet worden gebruikt en dienen te zijn uitgeschakeld.

SCADA-Operatoraccount
Een persoonlijk account dat wordt gebruikt voor de bediening van SCADA systemen
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-applicatiebeheeraccount
Een persoonlijk account dat wordt gebruikt om de applicatie op het SCADA systeem te beheren
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

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: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

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: 180 dagen
Wachtwoordlengte: minimaal 20 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

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: minimaal 8 karakters
Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 1 van elk.

CSR 7.2.4 Tips voor het omgaan met wachtwoorden
Enkele tips:

a. Gebruik een wachtwoord dat is gebaseerd op een zin, 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 voorbij en leggen alle vogels een ei!” wordt “Ahri5i4velavee!”, waarbij de maanden zijn vervangen door cijfers).
b. Gebruik 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: 3KleineKleutertjesdiezatenopeen###).
c. Gebruik een elektronische wachtwoordkluis die speciaal voor dit doel is ontwikkeld. Binnen RWS is Keepass 2 een goedgekeurde wachtwoordkluis. Enkele andere voorbeelden van veelgebruikte wachtwoordkluizen zijn Roboform, Dashlane, LastPass.

d. Als een wachtwoord in een elektronische wachtwoordkluis wordt opgeslagen, dan is een wachtwoord nodig om die applicatie te openen. Daarvoor geldt dezelfde wachtwoordrichtlijn voor het meest complexe opgeslagen wachtwoord in de kluis.
e. Gebruik voor je bedrijfs-account niet hetzelfde wachtwoord als voor je privéaccounts (bijvoorbeeld: persoonlijke gmail, facebook, ANWB site, bol.com, etc.).
f. Gebruik binnen het bedrijf niet overal hetzelfde wachtwoord. Gebruik een verschillend wachtwoord voor je gewone desktopomgeving, je bedienplek of je yammer account.
g. Deel je wachtwoord met niemand, tenzij dit is vereist volgens de procedures.
h. Wachtwoorden mogen nooit worden opgeschreven of digitaal worden opgeslagen zonder te zijn vercijferd.
i. Schrijf nooit een wachtwoord in e-mail, chat of ander communicatiemiddel.
j. Praat niet over je wachtwoord, geef geen hints over je wachtwoord aan anderen.
k. Indien een wachtwoord fysiek moet worden opgeslagen (bijvoorbeeld, omdat dat volgens een veiligheidsprocedure moet), sla het wachtwoord dan op in een fysieke kluis. Zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.

CSR 7.2.5 Wijzigen van wachtwoorden

Als het 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 en dit vast te leggen in een korte procedure.

Bijlage CSR 8 Patch management

CSR 8.1 Doelstelling

Vrijwel alle apparatuur aanwezig op een object heeft te maken met software en/of firmware. Om het aantal kwetsbaarheden in deze apparatuur tot een minimum beperkt te houden, is het van belang om de software en firmware up-to-date te houden en regelmatig te patchen. Deze richtlijn helpt Opdrachtnemers een effectief patch management regime op te stellen en te volgen, waarbij aandacht is voor de risicobeoordeling van de patch op de functies van het object en daarmee ook de business impact voor het (al dan niet) uitvoeren van patches.

CSR 8.2 Best practice

CSR 8.2.1 Bepalen van uit te rollen patches

Opdrachtnemers kunnen tenminste de volgende zaken in hun patch management procedures opnemen, om te bepalen welke patches relevant zijn voor het object en uitgerold dienen te worden:

a. Inventariseer voor het object welke software en firmware er op elk apparaat draait en neem dit op in het (bij voorkeur centrale) CMDB;
b. Houd bij welke kwetsbaarheden er zijn en worden ontdekt voor de systemen die in gebruik zijn. Beoordeel de risico's van de kwetsbaarheden voor het object (zie paragraaf CSR 8.2.2);
c. Houd bij welke patches er uitkomen voor alle apparaten en controleer welke relevant zijn. Indien patches een invloed kunnen hebben op de werking van (b.v. SCADA-) software, houdt bij welke patches zijn goedgekeurd door de leverancier;
d. Maak een alternatief mitigatievoorstel indien besloten wordt om een specifieke patch niet te installeren; Bepaal de risico's die overblijven indien wordt gekozen voor de alternatieve migratie;
e. Houd voor beheer en onderhoud een lijst bij met alle te installeren patches en de systemen waarop dit dient te gebeuren.

CSR 8.2.2 Risicobeoordeling

Zolang een kwetsbaarheid niet is verholpen door installatie van een patch of door een andere vorm van mitigatie, is er kans op misbruik van de kwetsbaarheid. Het risico hierop dient te worden bepaald. Dit gebeurt middels een risicobeoordeling. Hierbij worden kans en impact beschouwd.

Kans

De kans dat een kwetsbaarheid wordt uitgebuit is afhankelijk van de blootstelling van de kwetsbaarheid en de uitvoerbaarheid van het exploiteren van de kwetsbaarheid.

De kans dat de kwetsbaarheid wordt uitgebuit		Omschrijving kans en daarmee het benutten van de kwetsbaarheid
1	**Verwaarloosbaar** *t > 5 jaar*	De kans en daarmee het falen of misbruik van de functie van het object wordt niet binnen 5 jaar verwacht.
2	**Klein** (*3 jaar < t ≤ 5 jaar*)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht.
3	**Middelmatig** (2 *jaar < t ≤ 3 jaar)*	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht.
4	**Groot** (1 jaar < *t ≤ 2 jaar*)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht.
5	**Zeker** (*t ≤ 1 jaar)*	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen nu en 1 jaar verwacht.

Impact

Indien de kwetsbaarheid wordt uitgebuit dan heeft dit een bepaalde impact op het object. Deze impact dient te worden bepaald op basis van consequenties. Deze consequenties kunnen in verschillende categorieën van RAMSSHEEP liggen. De mee te nemen consequentiecategorieën zijn mede afhankelijk van het object. De categorie met de grootste impact consequentie wordt

overgenomen voor de risicomatrix en bepaalt uiteindelijk samen met de kans het risico die in de risicomatrix wordt weergegeven voor het object.

RAMSSHEEP

R: Reliability (Betrouwbaarheid)
A: Availability (Beschikbaarheid)
M: Maintainability (Onderhoudbaarheid)
S: Safety (veiligheid)
Se: Security (Beveiliging)
H: Health (Gezondheid)
E: Environment (Omgeving en Milieu)
€: Economics (Levensduurkosten)
P: Politics (Politiek)

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
R	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
A	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een minimale invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
M	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium verwaarloosbaar moelijker uitgevoerd kan worden binnen de randvoorwaarden van gebruik.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium minimaal moeilijker uitgevoerd kan worden binnen de randvoorwaarden van het gebruik.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen ernstige negatieve invloed heeft op de prestaties van de netwerkschakel.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen catastrofale negatieve invloed heeft op de prestaties van de netwerkschakel.

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
S	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft een verwaarloosbare invloed op gebruiksveiligheid van het object, maar dit blijft binnen geaccepteerde grenzen.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en leidt tot een situatie die de geaccepteerde grenzen voor gebruiksveiligheid benaderd en leidt daardoor tot een minimaal aantal extra ongelukken met tijdelijke gezondheidsschade of letsel zonder verzuim.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en leidt tot het niet voldoen aan gestelde eisen ten aanzien van gebruiksveiligheid wat daardoor leidt tot een ernstige toename van het aantal ongelukken met blijvend letsel of met blijvende gezondheidsschade.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft een catastrofaal negatief effect op de gebruiksveiligheid wat leidt tot extra dodelijk gevaar bij normaal gebruik.
Se	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object maar heeft een minimale invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffend object die tot security incidenten leiden en heeft hiernaast ernstige negatieve invloed op de hoofdfunctie.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object die tot security incidenten leiden en heeft hiernaast catastrofale negatieve invloed op de hoofdfunctie en of de prestaties van de netwerkschakel.
H	Het niet patchen heeft een verwaarloosbare negatieve invloed op de gezondheid.	Het niet patchen heeft een minimale negatieve invloed op de gezondheid.	Het niet patchen heeft een ernstige negatieve invloed op de gezondheid.	Het niet patchen heeft een catastrofale negatieve invloed op de gezondheid en veroorzaakt overlijden.
E	Het niet patchen heeft een verwaarloosbaar negatief effect op het gebruik.	Het niet patchen heeft een beperkt negatief effect op het gebruik en beperkt zich tot consequenties voor het lokale netwerk.	Het niet patchen maatregel heeft een ernstig negatief effect op het gebruik en heeft consequenties voor het regionale netwerk.	Het niet patchen heeft een catastrofaal negatief effect op het gebruik en heeft consequenties voor het landelijke netwerk.
€	Uitstel patch geeft < 50 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 500 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 1000 k Euro aan	Uitstel patch geeft > 1000 k Euro aan

	Impact			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
			extra onderhoudskosten.	extra onderhoudskosten
P	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft verder geen politieke consequenties.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor verscherpte controles door toezichthouders.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor negatieve media berichtgeving die tot kamer vragen kunnen leiden.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en de positie van DG, de Minister of Staatssecretaris staat ter discussie.

Risico
Het uiteindelijke risico wordt gepaald door het combineren van kans en impact in een risicomatrix.

		Impact			
		Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
Kans	Verwaarloosbaar (1)	Acceptabel (1)	Acceptabel (2)	Acceptabel (3)	Acceptabel (4)
	Klein (2)	Acceptabel (2)	Acceptabel (4)	Ongewenst (6)	Ongewenst (8)
	Gemiddeld (3)	Acceptabel (3)	Ongewenst (6)	Ongewenst (9)	Ongewenst (12)
	Groot (4)	Acceptabel (4)	Ongewenst (8)	Ongewenst (12)	Onacceptabel (16)
	Zeker (5)	Ongewenst (5)	Ongewenst (10)	Onacceptabel (15)	Onacceptabel (20)

De risicoscore wordt eenvoudig bepaald door kans- en impactscore met elkaar te vermenigvuldigen. De hoogte van dit getal geeft aan hoe noodzakelijk een beheersmaatregel in de vorm van een patch is. Hierin worden drie niveaus onderscheiden: onacceptabel (rood), ongewenst (oranje) of acceptabel (groen).

1. Onacceptabel — Risicoscore 15 t/m 20
Er moeten direct beheersmaatregelen worden getroffen om het risico te beheersen. Dat kan door de patch zo snel mogelijk te implementeren of minimaal (tijdelijk) compenserende maatregelen te treffen.
2. Ongewenst — Risicoscore 5 t/m 12
De patch moet worden doorgevoerd om het risico te beheersen ofwel worden aangetoond waarom dit nu niet haalbaar/noodzakelijk is. Een planning voor het doorvoeren van de patch is vereist naast tijdelijke compenserende maatregelen om zolang het risico te reduceren.
3. Acceptabel — Risicoscore 1 t/m 4
De patch hoeft niet direct doorgevoerd te worden en kan gewoon worden doorgevoerd binnen het geplande reguliere onderhoudsmoment van de systemen.

CSR 8.2.3 Inplannen van patches
Afhankelijk van de urgentie van de patches, kunnen deze tijdens regulier periodiek onderhoud worden geïnstalleerd. Hiertoe dient instructie te worden gegeven aan de monteur van Opdrachtnemer. Het is soms noodzakelijk apparatuur opnieuw op te starten na installatie van patches. Tijdens zulke herstarts is het mogelijk dat het object niet kan worden bediend. Inplannen van patches dient dan ook altijd te gebeuren in overleg met RWS.

CSR 8.2.4 Testen van patches
Om te voorkomen dat de uitrol van patches problemen geeft op het object, dienen patches vooraf te worden getest op werking en integriteit. Bij voorkeur gebeurt dit in een OTA-omgeving. Uitsluitend patches die dienen te worden geïnstalleerd dienen te worden getest.

CSR 8.2.5 Verantwoord uitrollen van ingeplande en geteste patches

Plan voor roll-back bij falende patches

a. Opdrachtnemer dient ervoor te zorgen dat er altijd en goed werkende back-up is, waarop kan worden teruggevallen indien een patch problemen geeft na installatie;
b. Opdrachtnemer kan overwegen een extra back-up te maken vlak voordat patches worden geïnstalleerd;
c. Opdrachtnemer dient gedurende de geplande onderhoudswerkzaamheden tijd te reserveren voor een eventuele roll-back van back-up op apparatuur.

Controleren of patches succesvol zijn uitgerold

a. Opdrachtnemer dient na de uitrol van de patch te controleren of de uitrol is geslaagd en goed is afgerond;
b. Indien de patch succesvol is uitgerold, dient Opdrachtnemer te controleren of de werking van het object niet is aangetast en of alle toepassingen nog functioneren als verwacht.

Controleren of systeem hardening niet is aangetast

a. Tot slot dient Opdrachtnemer te controleren of de mate van systeem hardening niet is aangetast door het installeren van de patch. Bijvoorbeeld:
    i. Zijn afgesloten poorten niet opengezet;
    ii. Zijn uitgeschakelde of verwijderde programma’s en/of DLL’s niet terug geïnstalleerd en geactiveerd;
b. Indien de hardening is aangetast, dient het niveau van hardening te worden hersteld.

Bijlage CSR 9 Hardening

CSR 9.1 Doelstelling

Hardening betreft het verwijderen of uitschakelen van overbodige en/of ongebruikte functionaliteit van een apparaat en is van toepassing op software, hardware en netwerk. Hardening zorgt ervoor dat systemen minder kwetsbaar zijn voor malware en minder snel gecompromitteerd kunnen worden. Hardening wordt toegepast op zowel IT als IA componenten.

Er worden drie methoden van hardening toegepast, te weten software hardening, hardware hardening en netwerk hardening:

a. Software hardening is van toepassing op operating systemen (bijvoorbeeld Microsoft Windows, Linux, iOS, Android) en applicaties (bijvoorbeeld HMI of engineering software, configuratietools, maar ook MS Office, Acrobat reader, Active-X controls en Adobe Flash);
b. Hardware hardening is van toepassing op bijvoorbeeld firmware, alsook het uitschakelen van niet gebruikte communicatiepoorten, antennes, en overige niet gebruikte functionaliteit;
c. Netwerk (Process Control Network) hardening is van toepassing op bijvoorbeeld uitschakelen van onveilige en niet gebruikte protocollen, het beperken van netwerkverkeer (firewalls) en segmentatie/zonering van het netwerk.

Maak indien mogelijk gebruik van de aanwezig security opties van de fabrikant/leverancier.

CSR 9.2 Best practices

CSR 9.2.1 Basistips

Enkele basistips voor hardening zijn:

a. Software
   i. Operating System;
      - De operationele OS versie dient altijd te worden ondersteund door de OS leverancier;
      - Gebruik waar mogelijk de nieuwste (mogelijke) versie[3];
      - Installeer de laatste (mogelijke) patches[1];
      - Schakel niet-gebruikte system services uit of verwijder deze[4];
   ii. Virtualization layer;
      - Gebruik de nieuwste (mogelijke) versie[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
      - Installeer de laatste (mogelijke) patches[1];
      - Schakel niet-gebruikte functionaliteit uit of verwijder deze;
   iii. Applicaties
      - Verwijder alle niet noodzakelijke applicaties;
      - Installeer de nieuwste versie van applicaties[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
      - Installeer de laatste (mogelijke) patches[1];
      - Zorg voor secure coding tijdens ontwikkeling van eigen software[5];
   iv. Firmware
      - Installeer de laatste (mogelijke) firmware[1];
b. Hardware
   v. Schakel niet-gebruikte poorten uit
      - Gebruik portblockers als niet-gebruikte poorten niet kunnen worden uitgeschakeld om abusievelijk gebruik te voorkomen en tamper-evident stickers (void stickers) om manipulatie te detecteren;

[3] Download alleen van gevalideerde vendorlocaties en controleer de integriteit van downloads middels een checksum.
[4] Zie ook Hardeningprofielen zoals hierna behandeld.
[5] Zie SSD document van CIP

- Beperk de gebruiksmogelijkheden van de nog openstaande poorten (bv. USB alleen voor hid (muis/keyboard)); Gebruik tamper-evident stickers (void stickers) om manipulatie te detecteren;

vi. Schakel niet noodzakelijke draadloze toegang uit (bv. WiFi, Bluetooth, IR, NFC, 4G, 5G, LoRa);

vii. Schakel niet gebruikte functionaliteit uit en verwijder deze waar mogelijk (bv. ingebouwde 4G/5G modem, antennes, I/O);

c. Netwerk

viii. Schakel niet-noodzakelijke communicatieprotocollen uit (bv. FTP, SMB, telnet);

ix. Pas netwerksegmentatie toe. Scheidt hierbij essentiële delen voor de besturing van niet essentiële delen;

x. Beperkt netwerkverkeer tussen verschillende netwerkzones middels firewalls.

CSR 9.2.2 Hardening-profielen

Op Internet zijn de nodige hulpmiddelen te vinden ter ondersteuning van het hardening-proces. Hardening (en tooling daarvoor) kan en mag alleen ingezet worden wanneer met zekerheid gesteld kan worden dat de inzet hiervan geen risico vormt voor de continuïteit van werking van het systeem. Het is van belang dit zowel vooraf als achteraf te testen.

Enkele van deze hulpmiddelen zijn:

CIS

De 'Security Benchmarks' van CIS heeft op internet standaard hardening-profielen beschikbaar voor de meeste platformen: http://www.cisecurity.org/

CIS Benchmarks: https://www.cisecurity.org/cybersecurity-best-practices/

Microsoft

Microsoft Security Baselines (Security Compliance Toolkit - SCT): https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

Microsoft Baseline Security Analyzer (MBSA): https://www.microsoft.com/en-us/download/details.aspx?id=19892

Defense Information System Agency (DISA)

Security Technical Implementation Guides (STIGs): https://public.cyber.mil/stigs/downloads/

Bijlage CSR 10 Logging

CSR 10.1 Doelstelling

Vanuit de BIO is logging vereist, waarbij de nadruk ligt op het vastleggen van gebruikershandelingen binnen applicaties, t.b.v. auditing. Deze logvereisten zijn vertaald naar logging voor IA systemen, waarbij de nadruk ligt op het systeemgedrag en –activiteiten. Logging binnen de IA-omgeving heeft dan ook meer betrekking op het waarborgen van beschikbaarheid en integriteit van de IA, door:

a. Het verzamelen, analyseren en reageren op status info van de ICT en ISC/SCADA deelsystemen binnen de IA;
b. Het ontdekken van menselijke fouten of systeem fouten, zoals fouten bij de bediening, maar ook het ontdekken van indringers in systemen;
c. Het ontdekken van corruptie van data of programmatuur;
d. Het ondersteunen van onderzoek na een incident.

CSR 10.2 Best practice

De volgende maatregelen sluiten aan bij de doelstelling van logging van IA systemen:

a. Een syslog server inrichten die de syslog events vanuit de gelaagd opgebouwde objectnetwerk verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen;
b. De syslogserver wordt voorzien van malware protectie, hardening en logging van de activiteiten op de server zelf (toegang, config/systeemaanpassingen en kopieer acties);
c. De syslogserver en syslog database is alleen toegankelijk voor geautoriseerden;
d. De syslog database kan niet gewijzigd of vernietigd worden door beheerders;
e. Het openen van een nieuw logbestand maar ook het verwijderen ervan dient te worden gelogd;
f. De bewaartermijn van de syslog database moet instelbaar zijn met een minimum van een maand;
g. Op aangeven van Opdrachtgever wordt de syslog database langer bewaard;
h. De syslog database dient zodanig ingericht te worden dat deze via het RWS netwerk toegankelijk is voor het Security Operations Centre van RWS;
i. De ICT en ICS/SCADA systemen die ingezet worden voor het object dienen de syslog gebeurtenissen door te geven aan de syslogserver voor vastlegging in de syslog database;
j. Het ICT of ICS/SCADA deelsysteem binnen de IA dat de logregel veroorzaakt staat vaak niet in de logregel zelf, in dat geval moet de syslog server deze toevoegen aan de opgenomen logregel;
k. Om meldingen goed te kunnen correleren is het essentieel dat tijdsynchronisatie (NTP) is ingericht. Hiervoor dient de interne tijdserver te worden gebruikt. Niet alleen de logserver dient te worden geconfigureerd op een tijdserver, maar ook alle aangesloten componenten zoals PLC's welke logregels genereren op de logserver;
l. Indien mogelijk dient Transport Layer Security (TLS) via TCP op poort 6514 gebruikt te worden (RFC 5425). Indien dit niet mogelijk is omdat de gebruikte apparatuur dit niet ondersteunt, kan gebruik gemaakt worden van UDP port 514 voor transmissie naar de logserver;
m. Voor zover de ICT en ICS/SCADA systeemcomponenten hierin voorzien dienen de volgende events aangeleverd te worden aan de syslogserver:

Event:	**Omschrijving:**
Log In	Succesvolle login (lokaal of op afstand)
Manual Log Out	Gebruiker logt zelf uit
Timed Log Out	Uitloggen door voor-ingestelde tijd (time-out)
Value Forcing	Handmatig aangepaste waarde (overschrijving)
Configuration Access	Download van de PLC configuratie naar datadrager

Event:	Omschrijving:
Configuration Change	Upload van de PLC configuratie naar de PLC
Firmware Change	Nieuwe firmware installatie op de PLC
ID/Password Creation or Modification	Creatie of modificatie van een gebruiker of wachtwoord
ID/Password Deletion	Wissen van een gebruiker en wachtwoord in de PLC
Audit Log Access	Toegang tot de logbestanden in de PLC
Time/Date Change	Datum/Tijd aanpassing van de PLC
Unsuccessful Login Attempt	Onjuiste inlog poging op de PLC
Reboot	Herstart van de PLC
Attempted Use of Unauthorized Configuration Software	Ongeautoriseerde poging tot toegang van de PLC configuratie
Invalid Configuration or Firmware Download	Ongeldige configuratie of firmware download
Unauthorized Configuration or Firmware File	Ongeautoriseerde configuratie of firmware bestand
Unexpected Time Signal Out of Tolerance	Onverwachte tijd/datum wijziging
Invalid Field Hardware Changes	Ongeldige hardware aangesloten

n. Het aanleverformaat voor de syslogserver is:
<timestamp> <IP> <Host> <facility> <Severity level> <message>

Voorbeeld:
<Oct 14 2015 22:09:12> <10.1.2.40> <123> <auth> <Alert> <Attempted Use of Unauthorized Configuration Software>

waarbij:

i. <timestamp> bij default tijd in het formaat ‘date "+%b %d %Y %H:%M:%S"’, zoals hierboven;
ii. <IP> IP adres van het device, bijvoorbeeld 10.1.2.40;
iii. <Host> hostnaam of ID van het busdevice, in dit voorbeeld “123” in geval van een computer de hostnaam van de computer;
iv. <facility> soort log gebeurtenis, bijvoorbeeld: kern, user, auth, syslog;
v. <Severity level> bijvoorbeeld Emergency, Alert, Critical, Error, Warning;
vi. <message> het syslog bericht, bijvoorbeeld: Attempted Use of Unauthorized Configuration Software;

Bijlage CSR 11 Malware scanning en opschoning middels een USB

CSR 11.1 Doelstelling

Malware besmettingen zijn vandaag de dag niet meer uit te sluiten. Derhalve worden voor de bescherming van ICT en IA systemen tegen malware oplossingen gevraagd. Bij nieuwbouw systemen dient vanaf het ontwerp hier voldoende aandacht en uitwerking aan gegeven te worden. Echter de maatregelen voor de detectie van en preventie tegen malware kunnen bij de ontwerpkeuzes dilemma's opleveren. In die situaties dient contact en afstemming gezocht te worden met de Opdrachtgever voor de uiteindelijke keuze. Ook kunnen er bestaande omgevingen zijn waar (nog) geen antimalware voorzieningen op de ICT en IA systemen zijn getroffen maar waar u meer zekerheid wilt verkrijgen over eventuele aanwezigheid van malware.

Het is van belang dat in deze gevallen malware gedetecteerd en opgeschoond kan worden, door medewerkers die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen.

CSR 11.2 Best practice

CSR 11.2.1 Randvoorwaarden

Een risico bij malware scanning en opschoning is dat wanneer er daadwerkelijk een besmetting heeft plaatsgevonden u niet vooraf weet in welke mate (of met welk soort malware) de computers zijn besmet. Het installeren van een conventionele antivirus oplossing brengt een nieuw risico met zich mee, indien de antivirus software een besmet bestand aantreft op de computer zullen de meeste antivirus software oplossingen (bij standaardinstellingen) deze bestanden proberen op te schonen, in quarantaine te plaatsen of te verwijderen. Dit is uiteraard onwenselijk aangezien de besmette bestanden mogelijk vitaal zijn of noodzakelijk voor de juiste werking voor de bediening van het object.

Randvoorwaarde is dat de ingezette oplossing voor malware scanning zo ingesteld wordt dat het alleen detecteert en rapporteert. Er mag niets verwijderd worden.

De volgende paragrafen schetsen een goede manier om het scannen aan te pakken.

CSR 11.2.2 Voorbereiden USB-stick met antimalware software

a. Gebruik **bij voorkeur een nieuwe USB stick** waar de malwarescan software op geïnstalleerd gaat worden;
b. Als extra beveiliging voor de USB-stick met antimalware software dient bij voorkeur een USB stick met **schrijfbeveiliging** (of een SD-kaart met schrijfbeveiliging, in combinatie met een SD-kaart lezer) gebruikt te worden. Door de schrijfbeveiliging te activeren voordat de USB-stick in het besmette systeem geplaatst wordt, wordt besmetting van de USB-stick voorkomen;
c. Scan de USB stick **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
d. De USB-stick moet **voor elk gebruik** voorzien worden van de juiste –en meest actuele- **antimalware** software en malwaredefinities.

Een voorbeeld van een dergelijke antimalware software is de vrij verkrijgbare software van ClamAV welke als portable applicatie kan worden geïnstalleerd op een USB stick en kan worden voorzien van updates op een andere computer.
Voor Windows computers kunt u bijvoorbeeld de nieuwste versie van ClamWin downloaden via http://nl.clamwin.com/ (Voor Linux computers is deze via de website http://www.clamav.net/ verkrijgbaar).

Installeer de software via het installatie programma op een USB stick en na dat de software is voorzien van de laatste versie antivirus definities kan de USB stick gebruikt worden op de object computers welke niet zijn aangesloten op internet.

Standaard staat ClamWin zo ingesteld dat een besmetting alleen zal worden gerapporteerd, indien u er zeker van bent dat een eventueel besmet bestand geen cruciale rol heeft voor de werking van het bedieningssysteem kunt u vanuit het programma het virus verwijderen.

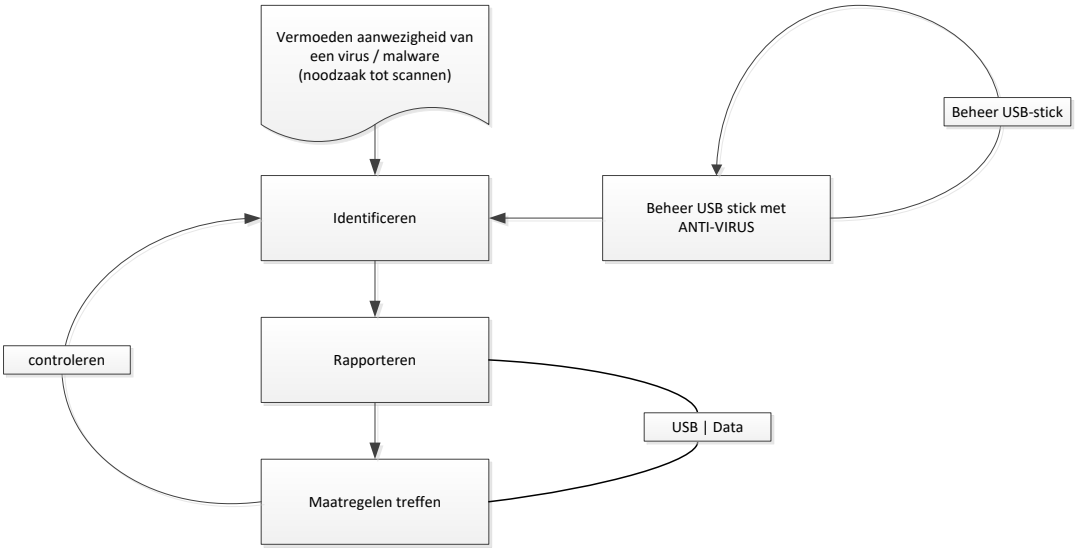
Uiteraard kunnen ook andere antimalware programma's worden gebruikt, mits zo ingesteld dat besmettingen uitsluitend worden gerapporteerd en niet in quarantaine worden geplaatst.

Om er zeker van te zijn dat alle bestanden kunnen worden gescand is het noodzakelijk het scanprogramma met verhoogde rechten op te starten. In Windows is dit "Als administrator starten" of "Run as administrator" en in Linux als "Root" of "Sudo".

CSR 11.2.3 Voorbereiden op malwarescanning
Handel volgens onderstaande werkwijze:

a. Update de USB stick met de laatste antimalware software en laatst beschikbare malwaredefinities;
b. Scan de USB stick met antimalware software **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
c. Zet op deze USB stick een malwarescan tool/software die **uitsluitend een rapportage** geeft over de besmetting zonder automatische handelingen;
d. Gebruik een malwarescanner welke **geen verbinding met internet** nodig heeft om op te kunnen starten (bijvoorbeeld i.v.m. licentie controle);
e. Gebruik een USB stick waar de antimalware software als een **portable applicatie** op kan worden geïnstalleerd;
f. De rapportage dient verzameld te worden op los media zoals een USB-stick. Gebruik hiervoor bij voorkeur een nieuwe andere stick dan die waarop de malwarescan software staat;
g. Scan de USB stick met antimalware software ook **na elk gebruik** op een computer buiten het object met een actuele malwarescan software.

CSR 11.2.4 Scannen en opschonen
In onderstaand schema wordt een bedoelde werkwijze getoond om een dergelijk object te schonen. Het proces kent de volgende stappen:



Identificeren
Gebruik de offline malwarescan tool om het systeem te controleren op virussen. Zorg voor correcte rapportage op een centrale plaats. Deze rapportage moet op een apart systeem weggeschreven worden, zodat het proces minimaal verstoord wordt.

Rapporteren
Verzamel de rapportage op aparte media zoals een USB-stick. Gebruik hiervoor bij voorkeur een **nieuwe andere stick** dan die waarop de malwarescan software staat.

Houdt ook bij de verzameling van rapportage rekening met voldoende controle op verwisselbare media: Bij plaatsen van een USB-stick in een besmet object is de kans op besmetting van de USB-stick reëel aanwezig. Herhaal hiertoe stap 6 van de instructie voorbereiding malwarescanning.

Maatregelen treffen
Bij constatering van malware dient in overleg met de objectbeheerder/eigenaar gekeken te worden naar mogelijke oplossingen voor het opschonen. Na autorisatie door de objectbeheer/eigenaar kunnen de te nemen stappen gepland en uitgevoerd worden. Houdt bij het treffen van de maatregelen weer rekening met de mogelijke besmetting van verwisselbare media. Extra aandachtspunt in dit geval is ook: Zorg dat de vervangen / vernieuwde bestanden (als daarvan sprake is) bij plaatsing niet besmet worden. Gebruik zo mogelijk checksums op bron en bestemming om de juistheid van de bestanden te controleren.

Controleren
Herhaal ter controle ten minste de eerste stap (Identificeren).

Bijlage CSR 12 Continuïteitsplan voor energievoorziening

CSR 12.1 Doelstelling

Het continuïteitsplan beschrijft per object de ingezette middelen voor continuïteit van de energievoorziening en acties die door de Opdrachtnemer moeten worden uitgevoerd om voorbereid te zijn op het herstel na stroomstoringen op objecten. In geval van omvangrijke stroomstoringen is het functioneren van de kritieke ICT en IA systemen geborgd.

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.

CSR 12.2 Best practice

Elk object heeft een eigen continuïteitsplan voor de energievoorziening. Een continuïteitsplan dient per object te worden opgesteld en tenminste het volgende te bevatten:

a. Risicoanalyse en afweging;
b. Overzicht van systemen, applicaties en services en back-up voorzieningen voor elektriciteit;
c. Overzicht van alle noodzakelijke systeemdocumentatie;
d. Organisatie en borging continuïteitsbeheer;
e. Periodieke beproeving en onderhoud van het continuïteitsplan voor energievoorziening.

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 de daarvoor benodigde energievoorzieningen in beeld te brengen.

Overzicht van systemen, applicaties en services en back-up voorzieningen

Dit betreft een overzicht van alle kritieke ICT en IA systemen, applicaties en services die operationeel moeten blijven in het geval van uitval van de primaire energie voorzieningen (zoals elektriciteit).

Overzicht van alle noodzakelijke systeemdocumentatie

Dit betreft een overzicht van actuele documentatie die benodigd is voor de noodvoorzieningen voor energie (bijvoorbeeld aansluittekeningen, gebruikshandleiding en procedures voor schakelen tussen noodstroomvoorziening en reguliere stroomvoorziening). De documentatie dient zowel digitaal als in hardcopy op twee fysiek gescheiden locaties bewaard te worden, waarbij wordt voldaan aan de gestelde eisen voor het omgaan met vertrouwelijke informatie.

Organisatie en borging continuïteitsbeheer energievoorziening

Dit betreft 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. Ook dient de afschaling te worden beschreven.

Periodieke beproeving en onderhoud van het continuïteitsplan voor energievoorziening

Dit betreft een beschrijving op welke wijze het continuïteitsplan minimaal jaarlijks wordt beproefd, alsmede een beschrijving van de wijze waarop het continuïteitsplan na iedere activering wordt geëvalueerd en geactualiseerd. Hierbij dient nadrukkelijk aandacht te worden besteed aan de werking van de (nood) energievoorzieningen en gerelateerde voorraden hiervan.

Bijlage CSR 13 Handelswijze bij SOC incident melding en verhoogde dreiging

CSR 13.1 Doelstelling SOC incidentmeldingen

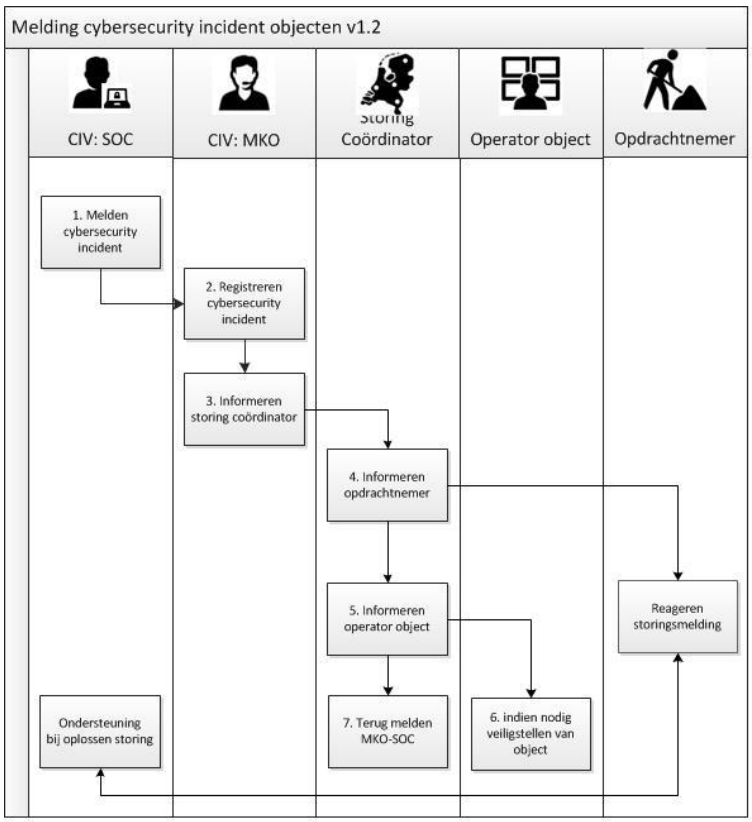
Het Security Operations Centre (hierna SOC) van Rijkswaterstaat ontwikkelt als één van haar diensten het monitoren van (loggings van) systemen en netwerkomgevingen van Rijkswaterstaat. Technische maatregelen worden ingevoerd om het ontsluiten en monitoren van (loggings op) regionale systemen en netwerkomgevingen mogelijk te maken. Resultaten worden door het SOC geanalyseerd, waardoor mogelijke cybersecurity incidenten vroegtijdig kunnen worden gesignaleerd.

Om bij aangetroffen cybersecurity incidenten zo snel mogelijk in te kunnen grijpen is het van belang deze direct te kunnen melden aan de eigenaar en/of de betreffende operator van het object. Hieronder volgt het proces voor meldingen van (mogelijke) cybersecurity incidenten aan de regio die vanuit het monitoringproces zijn ontdekt. In de regio worden cybersecurity incidenten ook cybersecurity storingen genoemd.

CSR 13.2 Algemeen

Na het ontdekken of vermoeden van een cybersecurity incident door het SOC meldt het SOC dit als een (mogelijk) cybersecurity incident aan de Missie Kritieke Ondersteuning (MKO). De MKO ontvangt de melding van het cybersecurity incident en registreert deze in Topdesk. Het MKO informeert op haar beurt de storing coördinator van de regio van het betreffende object. De storing coördinator informeert daarna de bedienaar en betreffende Opdrachtnemer van het object. Vervolgens wordt het al geïmplementeerde storingsmeldings en cybersecurity incident response proces gevolgd welke aansluit op het storingsproces van het object. Schematisch geeft dit de volgende processtappen.

CSR 13.3 Overzicht processtappen



CSR 13.4 RACI

In onderstaande RACI-matrix is voor elke activiteit aangegeven welke rollen welke verantwoordelijkheden hebben. Daartoe zijn per activiteit letters aan rollen toegekend. Zie voor de betekenis van elke letter de legenda onder de matrix:

Activiteiten Rapportage	**CIV: SOC**	**CIV: MKO**	**District: Storing coördinator**	**CNB: Operator object**	**Opdrachtnemer**	**Regio**
1. Melden cybersecurity incident	RA	I				
2. Registreren cybersecurity incident		RA				
3. Informeren storing coördinator		RA	I			
4. Informeren opdrachtnemer			RA	I	I	
5. Informeren operator object			RA	I		
6. Indien nodig veiligstellen van object			C	RA	C	C
7. Terug melden MKO – SOC	I	I	RA		C	

Legenda:

- R = Responsible:
  Degene (rol) die de activiteit uitvoert.
  Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- A = Accountable:
  Degene (rol) aan wie door de verantwoordelijke (R) verantwoording wordt afgelegd.
  Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- C = Consulted:
  Degene (rol) die een bijdrage kan leveren in het beoogde resultaat van de activiteit.
  Deze letter kan aan meerdere rollen worden toegekend.
- I = Informed:
  Degene (rol) die geïnformeerd wordt.
  Deze letter kan aan meerdere rollen worden toegekend.

CSR 13.5 Detailbeschrijving processtappen

1. Melden cybersecurity incident
Doel: constateren en melden van een (mogelijk) cybersecurity incident.

Het SOC monitort technische logging van objecten op (mogelijke) cybersecurity incidenten. Indien een (vermoeden van een) cybersecurity incident is geconstateerd dan meldt het SOC dit aan de MKO.
Indien het incident ernstig van aard is belt het SOC tevens de MKO om de doorlooptijd zo kort mogelijk te maken.
2. Registreren cybersecurity incident
Doel: het registreren van het (mogelijke) cybersecurity incident.

De MKO registreert het (mogelijke) cybersecurity incident in Topdesk aan de hand van de verkregen informatie van het SOC.

In de registratie legt de MKO vast:
- welk object het betreft.
- welk systeem (hostnaam) of welk netwerk (netwerknaam) het betreft.
- onder welk centraal meldpunt het object valt.
- korte beschrijving van het cybersecurity incident.
- behandelaarsgroep (kan ook het SOC zijn)
- de ernst van het cybersecurity incident (deze is standaard niet urgent)

3. Informeren storing coördinator
Doel: het infomeren van de storing coördinator over het (mogelijke) cybersecurity incident.

De MKO informeert de (aan het object gerelateerde) storing coördinator over het (mogelijke) cybersecurity incident. Daarbij worden de van het SOC verkregen gegevens over het (mogelijke) cybersecurity incident telefonisch doorgegeven en eventueel per mail bevestigd. Hierbij wordt duidelijk aangegeven dat het om een mogelijk cybersecurity incident gaat.

4. Informeren opdrachtnemer
Doel: het infomeren van de opdrachtnemer over het (mogelijke) cybersecurity incident.

De storing coördinator informeert de opdrachtnemer van het object waar het (mogelijke) cybersecurity incident is geconstateerd per telefoon.
De gegevens over het cybersecurity incident van het SOC worden hierbij doorgegeven. Een monteur van de opdrachtnemer gaat op pad om het gemelde cybersecurity incident nader te onderzoeken.

De storing coördinator registreert het cybersecurity incident van het SOC als storing in het beheerdermanagementsysteem, hierbij worden de van MKO ontvangen gegevens vastgelegd.

5. Informeren operator object
Doel: het infomeren van de operator over het (mogelijke) cybersecurity incident.

De storing coördinator informeert de operator van het object over het cybersecurity incident van het SOC en de in gang gezette actie om de monteur van de opdrachtnemer het incident te laten onderzoeken.

6. Indien nodig veiligstellen van object
Doel: voorkomen van ongevallen en incidenten.

De operator van het object stelt het object veilig indien de melding van het SOC daar aanleiding toe geeft.

7. Terug melden MKO – SOC
Doel: Het SOC kan contact leggen met de dienstdoende monteur.

De storing coördinator geeft de naam en telefoonnummer van de monteur door aan de MKO. De MKO legt deze gegevens vast in Topdesk en informeert daarmee het SOC. Het SOC kan vervolgens contact opnemen met de monteur om het cybersecurity incident toe te lichten en de monteur te ondersteunen.

Voorbeelden SOC cybersecurity incident meldingen

Het SOC kan in principe 8 verschillende meldingen (use cases) uit het systeem krijgen. Dit kan per object verschillen.

1. Mislukte autorisatie pogingen
2. Verboden protocollen geconstateerd
3. Poging uitgaand verkeer
4. Koppeling met KA geconstateerd
5. Malware virusmelding
6. Configuratie wijziging in beveiligingsinstellingen
7. Afwijkend remote beheer gedrag
8. Software, configuratie gewijzigd

In de melding wordt in ieder geval opgenomen:

- zo gedetailleerd als mogelijk welk object het betreft: sluis, eventueel welke kolk en/of hoofd, brug, spuiwerk, enz. .
- Welke melding het betreft, een van de 8 bovengenoemde meldingen, eventueel aangevuld met extra beschikbare informatie.
- Urgentie: in principe NIET urgent.

Standaard CS vragen aan de bedienaar:

- Heb ik toestemming gegeven voor het overnemen van mij IA-werkplek?
- Zie ik ongecontroleerde muisbewegingen en/of vensters open en dicht gaan?
- Zie ik ongecontroleerde bedienhandelingen van het object?
- Zie ik verkeerstekens van kleur wijzigingen zonder dat ik daar een handeling voor heb verricht?
- Zie ik objectbewegingen plaatsvinden zonder aanleiding, geen bewuste handeling?

CSR 13.6 Doelstelling verhoogde dreiging

Het is van belang dat de Opdrachtnemer tijdens een periode van verhoogde dreiging de juiste acties neemt om de risico's te mitigeren. Deze dreigingen vraagt om een specifieke handelswijze van medewerkers van de Opdrachtnemer die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen van Opdrachtgever.

CSR 13.7 Best practice voor verhoogde dreiging

Er is sprake van verhoogde dreiging als blijkt dat er een mogelijke (digitale) aanval op objecten van Rijkswaterstaat op handen is. Zo een aanval bevat mogelijk cyber elementen. Extra aandacht voor de ICT en IA systemen is daarom ook noodzakelijk. 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 Justitie en Veiligheid. Een aantal objecten van Rijkswaterstaat is vitaal en valt onder de meldplicht Wbni (Wet Beveiliging Netwerk- en Informatiesystemen) en Bbni (Besluit beveiliging netwerk- en informatiesystemen).

Indien er sprake is van een verhoogde cyberdreiging dan meldt het DCC-IenW (Departementaal Coördinatiecentrum Crisisbeheersing van het ministerie van Infrastructuur en Waterstaat) dit aan het lijnmanagement van Rijkswaterstaat, alsmede op welk specifiek object de dreiging mogelijk is gericht.

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

De Opdrachtnemer neemt de volgende acties:

a. De Opdrachtnemer neemt naar aanleiding van de storingsmelding contact op met de door Opdrachtgever aangegeven contractpersoon voor afstemming van uit te voeren acties en het tijdstip waarop deze acties nodig zijn;
b. 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 stand-by zijn om de objecten in dat verzorgingsgebied waar en indien nodig te 'servicen';
c. Indien de dreiging zich manifesteert in daadwerkelijke acties treed het incident response plan in actie.

Bijlage CSR 14 Incident response

CSR 14.1 Doelstelling

Indien een incident optreedt, is het van belang dat de Opdrachtnemer op efficiënte wijze hierop acteert. Om op uniforme wijze met incidenten om te kunnen gaan, dient Opdrachtnemer een incident response plan IA op te stellen. Dit plan beschrijft de te nemen stappen vanaf het optreden van het incident, tot aan het activeren van het recoveryplan en terugkeren naar de normale situatie. Het voorbereiden van de organisatie op herstel is geen onderdeel van incident response of herstel zelf en dient vooraf te worden uitgewerkt en uitgevoerd. Ook de herstelwerkzaamheden zelf die kunnen voorvloeien uit het incident vallen buiten de scope van dit plan en horen thuis in een apart recoveryplan.

Dit plan omvat de incident response als gevolg van een melding vanuit het SOC van RWS of cybercalamiteit op de IA-omgeving. Hierbij valt te denken aan een hack van een object, een (D)DoS aanval op een object, of de uitbraak van malware (b.v. cryptolocker malware). Er is mogelijk sprake van een cybercalamiteit op het object, als:

a. Het object in beweging is gebracht, zonder dat de bedienaar hier bewust opdracht toe heeft gegeven via de IA omgeving;
b. Fysieke acties op het object afwijken van de genomen acties binnen de IA omgeving/HMI;
c. Bediening en besturing werken niet zoals verwacht, of reageren helemaal niet;
d. Er verlies van controle of zicht is op de IA omgeving/HMI.

CSR 14.2 Best practices

CSR 14.2.1 Beoogd publiek voor het incident response plan IA

Het Incident Response Plan IA beschrijft het incident response plan van Opdrachtnemer voor de IA-omgeving van RWS. Dit document beschrijft de te nemen stappen om, tijdens het optreden van een incident op de IA systemen van een object, op een zo effectief mogelijke en veilige wijze te reageren op dit incident teneinde de gevolgen ervan zoveel mogelijk te beperken en daarna een effectief herstel mogelijk te maken.

Beoogd publiek voor dit document is:

a. Opdrachtnemer verantwoordelijk voor het operationeel houden van het object (Operations manager voor het object, security specialisten, bedienaars en onderhoudsmedewerkers);
b. RWS objecteigenaar;
c. RWS Security team (ter kennisgeving);
d. RWS SOC (i.v.m. adviserende rol).

Eenieder die een verantwoordelijkheid heeft in dit plan, dient een papieren versie van dit plan thuis op een veilige plek te bewaren.

CSR 14.2.2 Hoe dit plan te gebruiken

In geval een incident optreed op een object, dient het incident zo snel mogelijk te worden bedwongen, waardoor het incident niet kan escaleren en eventueel noodzakelijk herstel kan worden uitgevoerd. Dit incident response plan beoogt een basis te creëren waarmee Opdrachtnemer een verdere uitwerking kan doen welke specifiek is voor het object.

CSR 14.2.3 Incident response doelen voor het object

Primaire doelstelling van dit plan is incidenten op een efficiënte wijze te managen en controleren, waarna de IA-omgeving van een object in een werkende staat teruggebracht kan worden middels het recoveryplan. Dit incident response plan beoogt uitsluitend aanwijzingen te geven teneinde (cyber-) incidenten in de IA-omgeving van het object te managen.

De incident response doelen zijn als volgt geprioriteerd:

a. Detecteren dat een incident optreedt en een eerste analyse van de dreiging;
b. Insluiten van de dreiging en beheersen van het incident;
c. Bestrijden van de dreiging;

d. Communiceren met het recoveryteam;
e. Rapporteren.

Deze stappen zijn verder uitgewerkt in paragraaf CSR 14.2.5.

CSR 14.2.4 Incident Response organisatie

CSR 14.2.4.1 Rollen en verantwoordelijkheden
Het object heeft een incident response team, waarbij deelnemers afhankelijk van hun functie binnen de organisatie een rol bedeeld krijgen. Werknemers van zowel Opdrachtnemer als RWS zijn betrokken bij incident response, waarbij RWS een adviserende functie heeft.

Met betrekking tot het incident response team geldt het volgende:
a. Het incident response team bestaat uit belangrijke stakeholders binnen de Opdrachtnemer;
b. De stakeholders kennen en steunen het incident response plan;
c. Elke medewerker kan een incident melden aan het incident response team. Dit kan ook gebeuren door medewerkers van RWS, bijvoorbeeld het RWS SOC;
d. Elke deelnemer in het incident response team heeft een kaart met essentiële contactinformatie van het team en draagt deze bij zich;
e. Elke deelnemer in het incident response team bewaart een papieren kopie van het incident response plan thuis op een veilige plaats;
f. De rollen en verantwoordelijkheden van het incident response team dienen bekend te zijn bij eenieder die werkzaam is op of voor het object, zodat zij weten wie verantwoordelijk zijn voor incident response.

De volgende rollen kunnen worden onderkend binnen het incident response team:

Rol	**Verantwoordelijkheden**
Operations manager Opdrachtnemer voor het object	• Contact voor Incident Respons Organisatie; • Neemt contact op met RWS objecteigenaar bij eerste kennisname van incident; • Stemt af met RWS objecteigenaar.
RWS objecteigenaar	• Wordt geïnformeerd door Operations manager over incident en verwachte impact van de calamiteit; • Overleg met RWS SOC en RWS Security team m.b.t. impact en strategie voor mitigeren van het incident.
RWS SOC	• Kan incident melden aan Opdrachtnemer; • Is adviserend betrokken bij incident respons.
RWS Security team	• Kan adviserend worden betrokken bij incident response.
Security specialisten opdrachtnemer	• Onderzoek naar en afhandeling van het incident.
Bedienaars, onderhoudsmedewerkers	• Identificeren van incident; • Melden van incident aan operations manager; • Overleg met RWS security team en RWS SOC; • Rapporteren naar Opdrachtnemer.

CSR 14.2.4.2 Contactpersonen
Voor elk object dient een lijst met contactpersonen te worden opgesteld, voorzien van actuele contactgegevens. De tabel hierna kan worden gebruikt als template voor het opstellen van zo’n lijst.

Naam	**Functie**	**Mobiele nummer**	**Email**	**Opmerkingen**

Naam	Functie	Mobiele nummer	Email	Opmerkingen

CSR 14.2.5 Stappen in de incident response fase

CSR 14.2.5.1 Detecteren van het incident
Opdrachtnemer is verantwoordelijk voor het bedienen en onderhouden van het object. Op elk moment kan Opdrachtnemer een security incident opmerken. Dit kan zijn een incident op het IA netwerk, of een incident gerelateerd aan de procedures rondom cybersecurity. Ook kan een incident worden opgemerkt door RWS SOC, die het incident dan meldt aan Opdrachtnemer. Zodra een incident wordt gedetecteerd, wordt het incident response team van Opdrachtnemer actief voor een eerste analyse van de dreiging.

CSR 14.2.5.2 Eerste analyse van de dreiging
Het incident response team van Opdrachtnemer doet op basis van de eerste beschikbare gegevens over het incident een eerste analyse van de dreiging. Hierbij wordt het incident gecategoriseerd, op basis waarvan het incident binnen de organisatie wordt geëscaleerd en de securityorganisatie wordt opgeschaald.

CSR 14.2.5.3 Insluiten van de dreiging en beheersen van het incident
Gedurende deze fase wordt op basis van de eerste analyse besloten op welke wijze de dreiging wordt aangepakt. Hierbij kan het RWS SOC een adviserende rol spelen. Zodra de aanpak is vastgesteld, wordt de dreiging ingesloten zodat deze zich niet verder kan uitbreiden binnen of buiten het object. Op deze wijze wordt de dreiging onder controle gebracht zodat deze in de volgende fase bestreden kan worden. Het RWS SOC kan ook verzoeken om bestanden en systemen veilig te stellen voor mogelijk forensisch onderzoek. De instructies hiertoe dienen strikt opgevolgd te worden door Opdrachtnemer.

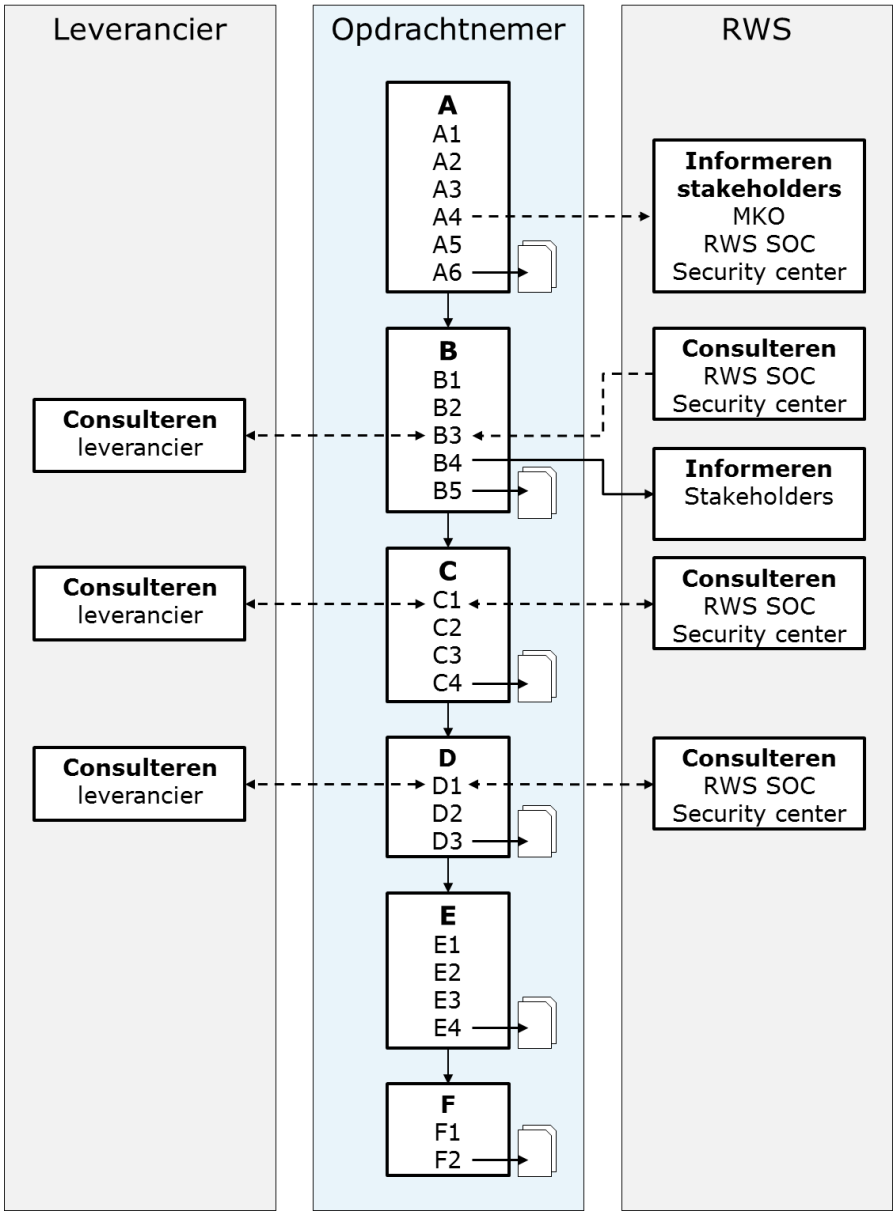
CSR 14.2.5.4 Bestrijden van de dreiging en beheersen van het incident
Het bestrijden van de dreiging wordt in algemeenheid uitgevoerd door het incident response team. In voorkomende gevallen is het bestrijden van de dreiging en incident alleen mogelijk tezamen met, of door herstel van het object. Het RWS SOC kan bij de beheersing van de dreiging en incident een adviserende en of sturende rol spelen.

CSR 14.2.5.5 Communiceren met het recoveryteam
Wanneer de dreiging bestreden is, of wanneer het incident volledig onder controle is, kan het recoveryteam aan de slag. Het recoveryteam zal in nauwe samenwerking met het incident response team de normale situatie gaan herstellen, waardoor het object weer volledig functioneel kan opereren. Het incident response team
informeert het herstel team over alle relevante informatie die over de dreiging beschikbaar is en mogelijk relevant is voor herstel.

CSR 14.2.5.6 Rapporteren
Zodra het recoveryteam aangeeft dat de normale situatie is hersteld, zal het incident response team het incident afsluiten en de rapportage daaromtrent afronden.

CSR 14.2.6 Incident response activiteiten

CSR 14.2.6.1 Inleiding
De activiteiten gedurende elk van de in de vorige paragraaf genoemde stappen zijn in de figuur hierna grafisch weergegeven en worden in de daaropvolgende paragrafen toegelicht.



CSR 14.2.6.2 Activiteit tijdens detecteren van het incident

Nr.	Activiteit	Omschrijving
A1	**Detectie incident**	Incident wordt gedetecteerd door systeem, Bedienaar, Onderhoudsmedewerker, RWS SOC, of …
A2	**Bevestigen incident**	Opdrachtnemer onderzoekt of het inderdaad een incident opgetreden is.
A3	**Informeren**	Indien er inderdaad een incident opgetreden is, wordt Operations manager geïnformeerd.
A4	**Beslissen opschaling**	Operations manager beslist of onmiddellijk wordt opgeschaald naar overige stakeholders, of dat eerst verdere analyse van de dreiging dient plaats te vinden.
A5	**Vervolgstappen**	Operations manager zorgt dat de vervolgstappen worden genomen zodat een eerste analyse van het incident wordt gedaan en de dreiging wordt ingesloten.

A6	**Rapporteren**	Maak de relevante gegevens betreffende detectie beschikbaar voor rapportage.

CSR 14.2.6.3 Activiteiten tijdens eerste analyse van de dreiging

Nr.	Activiteit	Omschrijving
B1	**Informeren**	Security specialist van Opdrachtnemer wordt geïnformeerd.
B2	**Analyseren**	Security specialist doet een eerste onderzoek naar het incident. Betreft het bijvoorbeeld malware, een cyberaanval (hack), een (D)DOS (Denial Of Service), of een poging tot verkrijgen van ongeautoriseerde toegang).
B3	**Consulteren**	Security specialist consulteert RWS SOC of leverancier indien nodig.
B4	**Informeren**	De resultaten van het onderzoek worden gebruikt om Operations manager te informeren, die op zijn beurt RWS informeert.
B5	**Rapporteren**	Maak de analyse van de dreiging beschikbaar voor rapportage.

CSR 14.2.6.4 Activiteiten tijdens insluiten van de dreiging en beheersen van het incident

Nr.	Activiteit	Omschrijving
C1	**Bepalen aanpak**	In samenspraak tussen security specialist van Opdrachtnemer, Operations manager en indien relevant RWS SOC, wordt besloten wat de beste aanpak is voor het insluiten van de dreiging.
C2	**Insluiten dreiging**	Acties worden uitgevoerd om ervoor te zorgen dat de dreiging wordt ingesloten en zich niet kan verplaatsen/uitbreiden. Hierbij kan bijvoorbeeld worden gedacht aan het isoleren van getroffen systemen, blokkeren van netwerkverbindingen, monitoring van communicatie.
C3	**Beheersen situatie**	Zodra de dreiging is ingesloten en de situatie onder controle is kan begonnen worden met de volgende stap, het bestrijden van de dreiging.
C4	**Rapporteren**	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.5 Activiteiten tijdens bestrijden van de dreiging en incident

Nr.	Activiteit	Omschrijving
D1	**Bepalen aanpak**	In samenspraak tussen security specialist van Opdrachtnemer, Operations manager en indien relevant RWS SOC, wordt besloten wat de beste aanpak is voor het bestrijden van de dreiging.
D2	**Bestrijden dreiging**	De stappen uit de aanpak worden gevolgd om de dreiging te bestrijden.
D3	**Rapporteren**	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.6 Activiteiten tijdens communiceren met het recoveryteam

Nr.	Activiteit	Omschrijving
E1	**Overdracht incident response --> herstel**	Draag alle beschikbare informatie uit de eerdere fasen van het incident response plan m.b.t. het incident over aan het recoveryteam.

E2	**Ondersteuning**	Ondersteun het recoveryteam met aanvullende informatie waar nodig.
E3	**Overdracht herstel -> incident response**	Verzamel informatie beschikbaar gesteld door het recoveryteam.
E4	**Rapporteren**	Maak de informatie beschikbaar voor rapportage.

CSR 14.2.6.7 Activiteiten tijdens rapporteren

Nr.	Activiteit	Omschrijving
F1	**Informatie verzamelen**	Verzamel alle informatie die beschikbaar is gemaakt voor rapportage.
F2	**Rapporteren**	Stel rapport op zodat het incident en de afhandeling ervan op een later moment geëvalueerd kan worden.

CSR 14.2.7 Testen en onderhoud van het incident response plan

CSR 14.2.7.1 Testen van het incident response plan
Voor het testen van het incident response plan geldt het volgende:

a. Het incident response plan dient bekend te zijn bij het incident respons team en het recoveryteam, zodat een ieder weet wat de verantwoordelijkheden zijn;
b. Door het incident response plan regelmatig te oefenen/testen raakt betrokken staf van verschillende organisaties (opdrachtnemer, RWS) op elkaar ingespeeld en kunnen betrokkenen snel en juist handelen in geval van nood;
c. Elk jaar dient het incident response plan als volgt te worden getest:
    i. Eén (1) volledige oefening. Gedurende deze oefening acteren alle betrokkenen alsof een echt cybersecurity incident is opgetreden en doorloopt men alle stappen van het incident response plan;
    ii. Twee (2) table top oefeningen. Hierbij kunnen afzonderlijke onderdelen van het incident response plan worden getest;
d. Oefeningen dienen te worden gedocumenteerd. Deze informatie dient te worden gebruikt als input tijdens de evaluatie van de oefening. Hierdoor:
    i. Leren betrokkenen wat goed ging, en vooral ook wat verbeterd kan worden;
    ii. Kunnen de geleerde lessen gebruikt worden om het plan te verbeteren en gedeeld worden met andere RWS objecten als best practice.

CSR 14.2.7.2 Onderhoud van het incident response plan
Het incident response plan dient periodiek te worden onderhouden. Ook na het testen van het incident response plan dient het plan te worden geëvalueerd, met aandacht voor het volgende:

a. Effectiviteit van het plan;
b. Volledigheid van het plan;
c. Aansluiting van het plan op de actuele situatie bij het specifieke object.

Het incident response plan dient te worden geactualiseerd, als:

a. Evaluatie van het plan hiertoe aanleiding geeft;
b. Een nieuwe Opdrachtnemer het beheer van een object op zich neemt;
c. Er een significante verandering is in de IA-omgeving van het object;
d. Er een significante verandering is in de consequentie van incidenten;
e. Er nieuwe middelen beschikbaar komen voor onderzoek naar en afhandelen van incidenten;
f. Er een significante verandering is in de risicomatrix voor het object.

Bijlage CSR 15 Recoveryplan

CSR 15.1 Doelstelling

Het is essentieel dat schade, ontstaan door het optreden van een incident, op effectieve wijze hersteld kan worden. Hiertoe dient de Opdrachtnemer een recoveryplan op te stellen. Dit plan beschrijft de hersteldoelen, rollen en verantwoordelijkheden, de verschillende fasen van herstel, herstelactiviteiten en het onderhouden van het recoveryplan.

Dit recoveryplan omvat het herstel van de IA-omgeving als gevolg van een cyber-calamiteit. Hierbij valt te denken aan een hack van een object, een (D)DoS aanval op een object, of de uitbraak van malware (b.v. cryptolocker malware).

Dit plan is opgesteld als een template voor Opdrachtnemers en dient als basis voor hen om een recoveryplan specifiek voor het object waarvoor zij verantwoordelijk zijn op te stellen. De initiële incident respons valt buiten de scope van dit plan en hoort thuis in een apart incident respons plan.

CSR 15.2 Best practices

CSR 15.2.1 Beoogd publiek voor het recoveryplan

Het recoveryplan IA-omgeving Objecten beschrijft de te nemen stappen om, na uitval van de IA systemen van een object door een cyberincident, dit object op een zo effectief mogelijke en veilige wijze weer operationeel te krijgen.

Beoogd publiek voor dit document is:

a. RWS objecteigenaar;
b. RWS Security team;
c. RWS SOC;
d. Opdrachtnemer verantwoordelijk voor het operationeel houden van het object (operations manager, medewerkers onderhoud).

Eenieder die een verantwoordelijkheid heeft in dit plan, dient een papieren versie van dit plan thuis op een veilige plek te bewaren.

CSR 15.2.2 Hoe het recoveryplan te gebruiken

In geval een object de beoogde functie niet meer kan vervullen als gevolg van een calamiteit, dient deze functie zo spoedig mogelijk te worden hersteld. Dit recoveryplan beoogt een basis te creëren waarmee Opdrachtnemers een verdere uitwerking kunnen doen welke specifiek is voor het object.

CSR 15.2.3 Hersteldoelen voor het object

Primaire doelstelling van dit plan is de IA-omgeving van een object terug te brengen in een werkende staat, waarbij veiligheid van personen en object voorop staan. Dit plan beoogt uitsluitend aanwijzingen te geven teneinde de IA-omgeving van het object te herstellen. Herstel van fysieke schade aan het object valt buiten de scope van dit recoveryplan. In het recoveryplan dient per systeem aandacht te zijn voor de Recovery Time Objective (RTO) en Recovery Point Objective (RPO), waarbij de laatste een relatie heeft met de back-up frequentie.

De hersteldoelen zijn als volgt geprioriteerd:

a. Herstel van functionaliteit van, en controle over, de veiligheidssystemen (safety);
b. Herstel van functionaliteit van, en controle over, de kritieke controle systemen binnen de IA-omgeving;
c. Herstel van functionaliteit van, en controle over, de overige controle systemen binnen de IA-omgeving;
d. Herstel van functionaliteit van, en controle over, de overige systemen binnen de IA-omgeving.

Onderstaande tabel kan door Opdrachtnemer worden gebruikt om een overzicht samen te stellen van de IA-systemen die binnen elke categorie vallen.

Prioriteit	Systeem categorie	Lijst met systemen binnen de categorie	Maximale hersteltijd
1	Safety/SIS	• .. • .. •	
2	Kritieke controle systemen	• .. • .. •	
3	Overige controle systemen	• .. • .. •	
4	Overige systemen	• .. • .. •	

Met safety systemen worden de systemen bedoeld die betrokken zijn bij de safety/ veiligheidsfuncties van het object. Onder kritieke controle systemen worden die systemen bedoeld die direct het primaire proces aansturen. Overige controle systemen zijn die systemen die niet direct betrokken zijn bij de aansturing van het primaire proces. Overige systemen zijn alle overige systemen binnen de IA-omgeving.

CSR 15.2.4 Recovery organisatie

CSR 15.2.4.1 Rollen en verantwoordelijkheden
Het object heeft een recoveryteam, waarbij deelnemers afhankelijk van hun functie binnen de organisatie een rol bedeeld krijgen. Werknemers van zowel Opdrachtnemer als RWS kunnen deelnemer zijn in de recovery organisatie.

Met betrekking tot het recoveryteam geldt het volgende:

a. Het recoveryteam bestaat uit belangrijke stakeholders binnen de organisatie;
b. De stakeholders kennen en steunen het recoveryplan;
c. Het recoveryteam heeft de risico's van het opereren onder het recoveryplan in kaart gebracht, samen met de extra mitigerende maatregelen om deze risico's terug te brengen;
d. Het recoveryplan kan alleen door daartoe bevoegde personen uit de recovery organisatie worden geactiveerd;
e. Communicatie binnen het team vind plaats via (waar relevant) Atex-proof portofoons en waar nodig voor gegevensuitwisseling, via email;
f. Elke deelnemer in het recoveryteam heeft een kaart met essentiële contactinformatie van het team en draagt deze bij zich;
g. Elke deelnemer in het recoveryteam bewaart een papieren kopie van het recoveryplan thuis op een veilige plaats;
h. De rollen en verantwoordelijkheden van het recoveryteam dienen bij eenieder die werkzaam is op of voor het object, zodat zij weten wie verantwoordelijk zijn voor herstel.

De volgende rollen kunnen worden onderkend binnen het recoveryteam:

Rol	Verantwoordelijkheden
Operations manager Opdrachtnemer voor het object	• Contact voor Incident Respons Organisatie; • Neemt contact op met RWS objecteigenaar bij eerste kennisname van incident; • Stemt herstel af met RWS objecteigenaar.
RWS objecteigenaar	• Wordt geïnformeerd door Operations manager over calamiteit, verwachte impact van de calamiteit en hersteltermijn; • Overleg met RWS SOC en RWS Security team m.b.t. impact en strategie voor herstel en overige continuïteitsmaatregelen.
Contactpersoon leverancier	• Wordt door Opdrachtnemer benaderd voor levering hardware/software/apparatuur indien dit niet (voldoende) voorradig is; • Levert hardware/software/apparatuur en ondersteuning aan Opdrachtnemer.
RWS SOC	• Is betrokken bij incident respons; • Beslist mede wanneer herstelwerkzaamheden kunnen worden uitgevoerd
RWS Security team	• Is betrokken bij incident respons; • Bewaakt namens RWS het recoveryproces.
Medewerker onderhoud	• Uitvoeren van de herstelwerkzaamheden; • Overleg met RWS security team en RWS SOC; • Rapporteren naar Opdrachtnemer.

CSR 15.2.4.2 Contactpersonen

Voor elk object dient een lijst met contactpersonen te worden opgesteld, voorzien van actuele contactgegevens. De tabel hieronder kan door Opdrachtnemer worden gebruikt om deze lijst samen te stellen.

Naam	Functie	Mobiele nummer	Email	Opmerkingen

CSR 15.2.5 Fasen van recovery

CSR 15.2.5.1 Voorbereiden op recovery

Om een spoedig herstel te kunne borgen is het van belang dat Opdrachtnemer hierop is voorbereid. Daarvoor is het noodzakelijk om de beschikking te hebben over actuele en relevante (systeem-)informatie van het object. Hieronder valt tenminste:

a. Geïnstalleerde hardware, inclusief firmware en configuraties;
b. Geïnstalleerde Operating Systems en software, inclusief configuraties;
c. Actuele back-ups van de systemen;
d. Netwerk configuratie, inclusief gebruikte communicatiemiddelen;
e. Documentatie (online en offline);
f. Recoveryorganisatie en communicatieplan;
g. Recoverymiddelen en werkprocedures;
h. Testprocedures;
i. Inbedrijfstellingsprotocollen.

CSR 15.2.5.2 Optreden van calamiteit

Deze fase begint met het optreden van de calamiteit. Gedurende de calamiteit treedt het incident respons plan in werking. Het incident respons plan houdt zich vooral bezig met de eerste reactie op de calamiteit en de afhandeling daarvan. Belangrijke activiteiten gedurende deze fase zijn

vaststellen van de calamiteit, notificatie van het management Opdrachtnemer en RWS, incident respons activiteiten en waar nodig inschakelen van RWS SOC. Deze activiteiten vallen buiten de scope van dit document.

CSR 15.2.5.3 Activeren van het recoveryplan
Gedurende deze fase wordt het recoveryplan geactiveerd. Gedurende deze fase worden betrokkenen (Opdrachtnemer, RWS en mogelijk leveranciers) geïnformeerd en dienen zij actief hun rol te vervullen in het recoveryplan. Het recoveryplan wordt geactiveerd slechts nadat de calamiteit is beheerst. Het nemen van eventuele noodmaatregelen voor continuïteit kan parallel lopen aan het recoveryplan. Deze noodmaatregelen voor bedrijfscontinuïteit van het object vallen buiten de scope van dit document.

CSR 15.2.5.4 Activiteiten m.b.t. recovery
Gedurende de recoveryfase dienen een aantal activiteiten te worden verricht. Deze activiteiten zijn, op hoofdpunten:

a. Vaststellen schade en benodigde acties t.b.v. recovery;
b. Recoveryactiviteiten t.b.v. netwerkapparatuur;
c. Recoveryactiviteiten t.b.v. veiligheidsvoorzieningen;
d. Recoveryactiviteiten t.b.v. machinebesturing;
e. Recoveryactiviteiten t.b.v. bediening en beheer;
f. Recoveryactiviteiten t.b.v. overige systemen.

Deze activiteiten worden in paragraaf CSR 15.2.6 verder uitgewerkt.

CSR 15.2.5.5 De-escalatie naar normale operationele status van het object
Op het moment dat alle activiteiten voor recovery zijn afgerond en het object weer werkzaam is, dient de normale operationele status van het object weer te worden bereikt. Dit gebeurt door het overdragen van de installatie door het recoveryteam aan het operationele team.

Met deze de-escalatie wordt het beheer en de bediening van het object teruggegeven aan de operatie. Het recoveryteam kan vervolgens het recoveryplan afsluiten met de benodigde rapportage.

CSR 15.2.6 Recoveryactiviteiten

CSR 15.2.6.1 Inleiding
De recoveryactiviteiten worden hierna toegelicht. Deze bevatten de stappen die genomen dienen te worden als onderdeel van het recoveryplan, zoals besproken in paragraaf CSR 15.2.5.4.

CSR 15.2.6.2 Recoveryactiviteit netwerkapparatuur

Nr.	Activiteit	Omschrijving
A1	**Uitvoeren risico- en impactanalyse**	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
A2	**Vervang defecte hardware**	Indien defecte hardware aanwezig, dient deze vervangen te worden door reserve exemplaren.
A3	**Laad de configuratiefiles**	Zet de laatste back-ups van de apparaat configuraties terug op de betreffende apparaten.
A4	**Check de configuraties**	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
A5	**Test de systemen op juiste werking**	Doe een regressietest op functionaliteit en connectiviteit.
A6	**Bijwerken back-ups**	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
A7	**Bijwerken CMDB**	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.

Nr.	Activiteit	Omschrijving
A8	**Rapporteren**	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.3 Recoveryactiviteit veiligheidsvoorzieningen

Nr.	Activiteit	Omschrijving
B1	**Uitvoeren risico- en impactanalyse**	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
B2	**Vervang defecte hardware**	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
B3	**Restore de software**	Zet de laatste backups van de systemen terug op de betreffende systemen.
B4	**Check de configuraties**	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
B5	**Test de systemen op juiste werking**	Doe een regressietest op functionaliteit en connectiviteit.
B6	**Bijwerken backups**	Maak, indien nodig, nieuwe backups en leg dit vast in het software beheersysteem.
B7	**Bijwerken CMDB**	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.
B8	**Rapporteren**	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.4 Recoveryactiviteit PLC's, VSD/VFD, smart sensors

Nr.	Activiteit	Omschrijving
C1	**Uitvoeren risico- en impactanalyse**	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
C2	**Vervang defecte hardware**	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
C3	**Restore de software**	Zet de laatste back-ups van de systemen terug op de betreffende systemen.
C4	**Check de configuraties**	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.
C5	**Test de systemen op juiste werking**	Doe een regressietest op functionaliteit en connectiviteit.
C6	**Bijwerken back-ups**	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
C7	**Bijwerken CMDB**	Logboek en configuratiewijzigingen (hard- en software) verwerken in CMDB.
C8	**Rapporteren**	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.5 Recoveryactiviteit HMI, SCADA, EWS, OWS, computerapparatuur

Nr.	Activiteit	Omschrijving
D1	**Uitvoeren risico- en impactanalyse**	Bepaal de risico's en mogelijke impact van de uit te voeren recoverywerkzaamheden.
D2	**Vervang defecte hardware**	Indien defecte hardware aanwezig, dient deze eerst vervangen te worden door reserve exemplaren.
D3	**Restore de software**	Zet de laatste back-ups van de systemen terug op de betreffende systemen.
D4	**Check de configuraties**	Loop de configuratie na van de betrokken systemen. Denk aan IP instellingen, accountinstellingen, rechten, hardening, etc.

D5	**Test de systemen op juiste werking**	Doe een regressietest op functionaliteit en connectiviteit.
D6	**Bijwerken back-ups**	Maak, indien nodig, nieuwe back-ups en leg dit vast in het software beheersysteem.
D7	**Bijwerken CMDB**	Logboek en wijzigingen (hard- en software) verwerken.
D8	**Rapporteren**	Stel rapport met bevindingen en aanbevelingen op.

CSR 15.2.6.6 Recoveryactiviteit overige systemen
Veel overige systemen zoals bijvoorbeeld een telefooncentrale en de CCTV installatie zijn leverancier specifieke installatiedelen en alleen door de leverancier zelf in te richten. Wij verwijzen daarvoor dan ook naar de specifieke leveranciers.

CSR 15.2.6.7 Testen van het recoveryplan
Voor het testen van het recoveryplan geldt het volgende:

a. Het recoveryplan dient bekend te zijn bij het incident respons team en het recoveryteam, zodat een ieder weet wat de verantwoordelijkheden zijn;
b. Door het recoveryplan regelmatig te oefenen/testen raakt betrokken staf van verschillende organisaties (opdrachtnemer, RWS, leverancier) op elkaar ingespeeld en kunnen betrokkenen snel en juist handelen in geval van nood;
c. Elk jaar dient het recoveryplan als volgt te worden getest:
    i. Eén (1) volledige oefening. Gedurende deze oefening acteren alle betrokkenen alsof een echt cybersecurity incident is opgetreden en doorloopt men alle stappen van het recoveryplan;
    ii. Twee (2) table top oefeningen. Hierbij kunnen afzonderlijke onderdelen van het recoveryplan worden getest;
d. Oefeningen dienen te worden gedocumenteerd. Deze informatie dient te worden gebruikt als input tijdens de evaluatie van de oefening. Hierdoor:
    iii. Leren betrokkenen wat goed ging, en vooral ook wat verbeterd kan worden;
    iv. Kunnen de geleerde lessen gebruikt worden om het plan te verbeteren en gedeeld worden met andere RWS objecten als best practice.

CSR 15.2.6.8 Onderhoud van het recoveryplan
Het recoveryplan dient periodiek te worden onderhouden. Ook na het testen van het recoveryplan dient het plan te worden geëvalueerd, met aandacht voor het volgende:

a. Effectiviteit van het plan;
b. Volledigheid van het plan;
c. Aansluiting van het plan op de actuele situatie bij het specifieke object.

Het recoveryplan dient te worden geactualiseerd, als:

a. Evaluatie van het plan hiertoe aanleiding geeft;
b. Er een significante verandering is in de IA-omgeving van het object;
c. Er een significante verandering is in de consequentie van incidenten;
d. Er een significante verandering is in de risicomatrix voor het object.

Bijlage CSR 16 Registratie assets in een configuratiemanagement database (CMDB)

CSR 16.1 Doelstelling

Het doel van een *Data model CMDB Cybersecurity Industriële Automatisering* is het vastleggen van heldere en eenduidige afspraken over de gegevensvastlegging en de uitwisseling ervan. In een (conceptueel/logisch) datamodel wordt vastgelegd over welke dingen we een administratie bijhouden: de entiteitentypes/Asset-types. Daarbij beschrijft dit model wat we hierover vastleggen: attribuuttypes en relatietypes.

Aanvullend op dit model wordt het *CMDB Cybersecurity Industriële Automatisering Excel Format* beschikbaar gesteld. Deze bevat aanwijzingen en templates om de gegevens in het voor u liggende model aan te leveren.

CSR 16.1.1 Scope

Het Data model CMDB Cybersecurity Industriële Automatisering kan worden gezien als een gedetailleerde beschrijving van de informatiebehoefte van de objecteigenaren in het kader van assetmanagent en het Security Operation Center (SOC). Het model stelt wel eisen aan de database(s) waarin de betreffende Asset-types worden vastgelegd maar bepaalt niet in welke database(s) dit zou moeten gebeuren.
In dit model worden per Asset-type de verplicht in te vullen velden beschreven. Waar de velden optioneel zijn, wordt dit expliciet aangegeven. Voor ieder veld geldt, dat deze verplicht moet worden ingevuld tenzij wordt vermeld dat het veld optioneel is.

CSR 16.1.2 Disclaimer

Het opslaan en beheren van documenten, behoort niet tot de scope van het *Data model CMDB Cybersecurity Industriële Automatisering*. Echter, voor vier Asset-types beschreven in dit model (Beheer en onderhoudsdocumentatie, Data- communicatienetwerkontwerp, Programmatuurbeschrijving en Wijzigingendocument) geldt wel dat deze naar documentatie verwijzen. De attribuuttypes betreffen dus specifieke metadata bij deze documentatie die voor Cybersecurity van belang is.
Voldoen aan de eisen van dit model betekent nog niet dat voor de betreffende documentatie aan alle wettelijke eisen m.b.t. de metadata voor documentatie is voldaan.

Dit model maakt waar mogelijk gebruik van standaarden zoals de Rijkswaterstaat Objecttypenbibliotheek (OTL), DISK en de NEN.

CSR 16.1.3 Beheer en Eigenaarschap

Het model wordt beheerd door het IV Configuratie Management Overleg (ICMO). Wijzigingen die betrekking hebben op de datamodellering of andere aanpassingen van het proces of procedures of functionele eisen van de tooling worden alleen op basis van een Request for Change (RFC) besproken.

CSR 16.1.4 Wijzigingsverzoeken

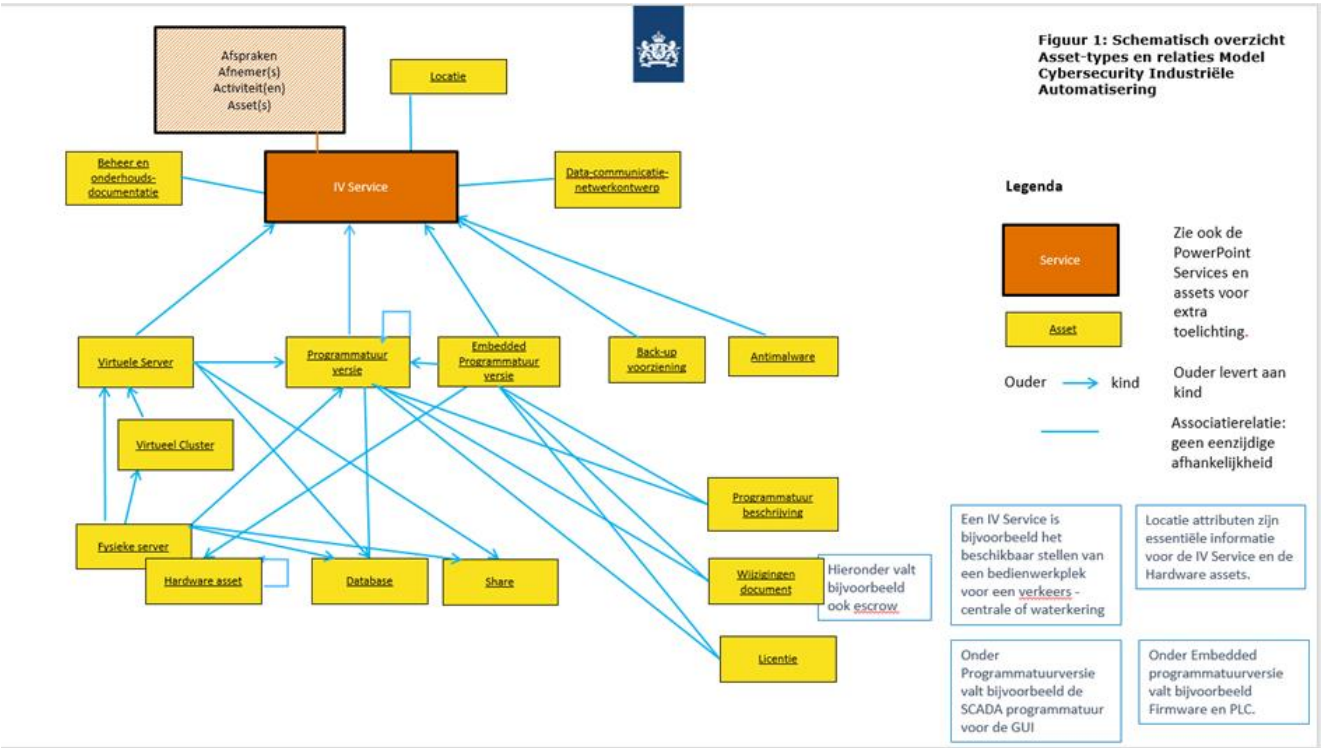
Het Data model CMDB Cybersecurity Industriële Automatisering bevat een overzicht van nu bij Rijkswaterstaat bekende, voor Cybersecurity relevante, Asset-types en attribuuttypes. Het is echter mogelijk dat de opdrachtnemer relevante assets beheert of levert die nog niet in dit model staan beschreven en wat betreft functionaliteit ook niet vergelijkbaar zijn. Dit vraagt een aanvulling op het voor u liggende model en de bovengenoemde templates.
Wanneer er een wijzigingen van het datamodel nodig is (bijvoorbeeld de toevoeging of verwijdering van een Asset-type), wordt deze wijziging voorgelegd aan de contactpersoon bij RWS en pas na schriftelijke goedkeuring door de aangewezen contactpersoon bij RWS doorgevoerd in de templates. Daarbij levert de opdrachtnemer een beschrijving van de betreffende wijziging zodat deze ook kan worden doorgevoerd in het Data model CMDB Cybersecurity Industriële Automatisering. Indien de wijziging toch vragen oproept bij relevante RWS medewerkers, wordt de wijziging toegelicht en zo nodig aangepast totdat deze door de betreffende RWS als begrijpelijk wordt ervaren.

CSR 16.1.5 Toekomst
Dit model is een éérste stap en zal met nieuwe kennis worden bijgewerkt.

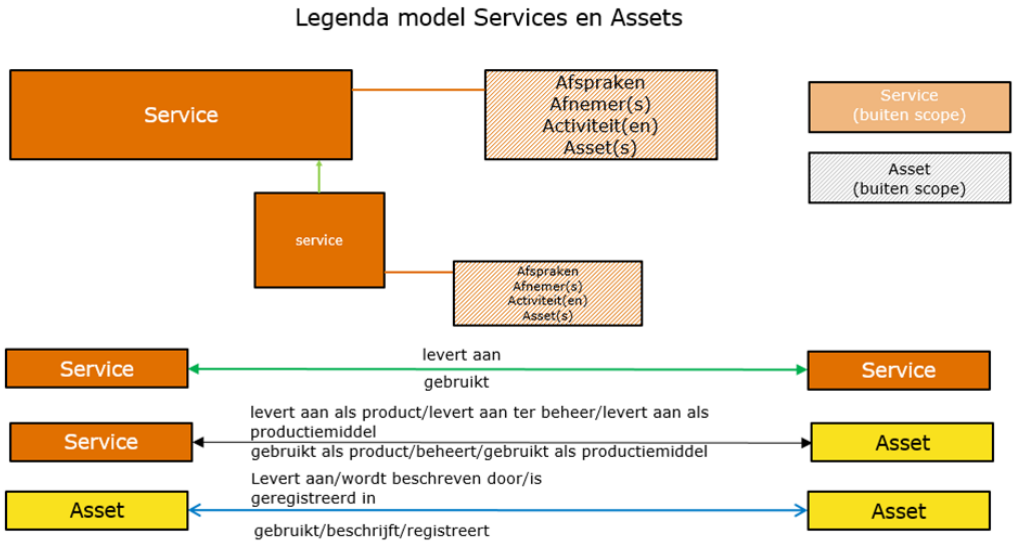
CSR 16.1.6 Leeswijzer
Paragraaf CSR 16.2 geeft een overzicht van de Asset-types en Relatietypes van het *Data model CMDB Cybersecurity Industriële Automatisering*. Paragraaf CSR 16.2.1 start met het schematisch overzicht. Begrippen uit dit overzicht worden daaropvolgend toegelicht in de paragraaf 16.2.2 *Samenvatting Metamodel Services, Assets en Relaties*. In paragraaf 16.2.3 volgt een beschrijving van de Asset-types en Relatietypes. Deze start met overzichten van de Assettypes (paragraaf 16.2.3.1) en de Relatietypes (paragraaf 16.2.3.2) Tot slot is voor alle Asset-types is een korte definitie opgesteld en worden de attribuuttypes beschreven. Dit is beschreven in de paragraaf Asset-types uitgelicht (deel 16.2.3.3).

CSR 16.2 Overzicht Asset-types en Relatietypes

CSR 16.2.1 Schematisch overzicht



CSR 16.2.2 Samenvatting Metamodel Services, Assets en Relaties



Service: een afgebakende prestatie van een persoon of organisatie, die voorziet in een behoefte van haar afnemers.

- Een service levert meestal één of meerdere assets als producten of beheert één of meerdere assets als beheerde objecten.
- Een service kan samengesteld zijn.
- Als een service een product levert, is het gespecificeerd welk product of producten het zijn en onder welke condities ze geleverd worden.
- Als een service een asset beheert, is het gespecificeerd welk asset of assets het zijn en onder welke condities ze worden beheerd. Denk bijvoorbeeld aan service levels.

Voorbeeld: beschikbaar stellen Bedienwerkplek
Voorbeeld: beschikbaar stellen transformatie door Noodsluit startautomaat

Asset: iets wat waarde vertegenwoordigd

- Een asset kan verschillende rollen vervullen afhankelijk van het gezichtspunt:
- Een asset kan een product zijn. Deze wordt dan geleverd aan derden voor gebruik of afgeleverd, om te behouden (verbruik).
- Een asset kan een productiemiddel zijn en wordt dan gebruikt door de dienstverlener.
- Een asset kan een beheerd object zijn.

In het *Data model CMDB Cybersecurity Industriële Automatisering* worden twee soorten relaties beschreven:

1. Relaties waarbij geen eenzijdige afhankelijkheid geldt: ***Associatierelaties.***

2. Relaties met een ***levert aan-gebruikt/Ouder-Kind relatie***

In de huidige CMDB van RWS vastgelegd als een levert aan/Ouder-Kind relatie waarbij de Ouder levert aan het Kind. Deze relatie kent 1 richting: van Ouder naar Kind.
Waarbij de pijl van de Ouder richting het Kind gaat.

Indien van toepassing, moeten de relaties worden vastgelegd als levert aan-gebruikt/Ouder-Kind relaties. Dit omdat juist het in beeld krijgen van de afhankelijkheden tussen assets en services één van de belangrijkste doelen is van dit model.

Aanvullende opmerkingen:
De in een Service Management Database en/of CMDB geregistreerde service, betreft altijd een instantie van de service:
een specifieke service die aan een specifieke afnemer/klant wordt geleverd. De omschrijving van de Service, die vele instanties kan hebben, word vastgelegd in de Servicecatalogus.
Het in de CMDB geregistreerde asset, betreft altijd een instantie van het entiteittype/assettype die een rol heeft in de instantie van één of meerdere service(s).
De omschrijving van het assettype, dat dus vele instanties kan hebben, wordt vastgelegd in het Conceptueel Datamodel Configuratie management waarvan het *Data model CMDB Cybersecurity Industriële Automatisering* een deelmodel is.

CSR 16.2.3 Beschrijving Asset-types en Relatietypes

CSR 16.2.3.1 Overzicht Asset-types

Model	**Asset-type**
Data model CMDB Cybersecurity Industriële Automatisering	Antimalware
Data model CMDB Cybersecurity Industriële Automatisering	Back-up voorziening
Data model CMDB Cybersecurity Industriële Automatisering	Beheer en onderhouds-documentatie
Data model CMDB Cybersecurity Industriële Automatisering	Data-communicatie-netwerkontwerp
Model Infra en Hardware KA	Database
Model Infra en Hardware KA	Embedded Programmatuurversie
Model Infra en Hardware KA	Fysieke Server
Model Infra en Hardware KA	Hardware asset
Model Generieke Eniteittypes	IV Service
Model Infra en Hardware KA	Share
Model Generieke Entiteittypes	Locatie
Model Programmatuur	Licentie
Data model CMDB Cybersecurity Industriële Automatisering	Programmatuur beschrijving
Model Programmatuur	Programmatuurversie
Model Infra en Hardware KA	Virtueel Cluster
Model Infra en Hardware KA	Virtuele server
Data model CMDB Cybersecurity Industriële Automatisering	Wijzigingen document (Escrow)

CSR 16.2.3.2 Overzicht Relatie types

Relatietype	Assettype/Servicetype-1	Is ouder van/levert aan	Assettype/servicetype-2
Ouder-Kind (Parent-Child) relatie	Virtuele Server		IV Service
	Virtuele Server		Programmatuur versie
	Virtuele Server		Database
	Virtuele Server		Share
	Programmatuur versie		IV Service
	Embedded Programmatuur versie		IV Service
	Back-up voorziening		IV Service
	Antimalware		IV Service
	Programmatuurversie		Programmatuurversie
	Fysieke server (Hardware asset)		Programmatuurversie
	Fysieke server (Hardware asset)		Database
	Fysieke server (Hardware asset)		Share
	Fysieke server (Hardware asset)		Virtueel Cluster
	Fysieke server (Hardware asset)		Virtuele Server
	Virtueel Cluster		Virtuele Server
	Embedded Programmatuur versie		Programmatuur versie
	Embedded Programmatuur versie		Hardware asset
	Hardware asset		Connection Type
	Netwerkcomponent (Hardware asset)		Connection Type
	Connection Type		Hardware assets (Fysieke serverpoort)
	Hardware asset		Hardware asset
	Zie voor de verdere mogelijke relaties van Hardware assets het model Infra & Hardware KA		

Assettypes met associatierelaties			
Relatietype	Assettype/Servicetype 1	Is verbonden met	Assettype/Servicetype 2
Associatierelatie	Beheer en onderhoudsdocumentatie		IV Service
	Data-communicatie-netwerkontwerp		IV Service
	Locatie Let op: locatiegegevens worden voorlopig als attribuuttypes bij IV Service geregistreerd		IV Service
	Programmatuurversie		Database
	Locatie Let op: locatiegegevens worden voorlopig als attribuuttypes bij assets geregistreerd		Hardware asset
	Programmatuur beschrijving		Programmatuur versie
	Programmatuur beschrijving		Embedded Programmatuur versie

	Wijzigingen document (Escrow)		Programmatuur versie
	Wijzigingen document (Escrow)		Embedded Programmatuur versie
	Licentie		Programmatuur versie
	Licentie		Embedded Programmatuur versie

CSR 16.2.3.3 Asset-types uitgewerkt

Hieronder volgt een gedetailleerde uitwerking van de in paragraaf 1.2 beschreven Asset-types.

Antimalware Asset-type

Product met functionaliteit voor bescherming tegen alle vormen van Malicious software.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		Unieke ID (Uniek ID zoals geregistreerd bij opdrachtnemer)
Status Programmatuur versie		Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Merk	Uit het Model Infra & Hardware KA: De handelsnaam, waaronder een producent een productrange op de markt plaatst.	
Producent	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	
Productnaam	Naam van het product, 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 programmatuur zoals uitgegeven door de producent
Ordernummer vendor		
Taal	Taalcode van de software conform ISO-693-3	Taalcode van de software conform ISO-693-3
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	keuzelijst: COTS, MOTS (modified of the shelf), maatwerk

A/B/C klassificatie	[A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig. Vastgesteld door RWS-bestuur.	[A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig.
Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		
GPS Location Lattitude		
GPS Location Longtitude		
RD X- coördinaat		
RD Y- coördinaat		

Back-up voorziening Asset-type

Product dat de functionaliteit biedt om een kopie te maken van de programmatuur. Het betreft hier twee eisen:

1. Er moet periodiek een back-up worden gemaakt.
2. Daarbij moet periodiek worden getest of de back-up voldoet voor een goede recovery. Zijn de media bijvoorbeeld leesbaar? De resultaten van die test moeten ook worden vastgelegd.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		Unieke ID (Uniek ID zoals geregistreerd bij opdrachtnemer)
Locatie laatste Back-up	Fysiek adres	
Datum laatste Back-up		d-m-jjjj (let op: streepjes noodzakelijk)
Datum laatste recovery test		d-m-jjjj (let op: streepjes noodzakelijk)
Recovery succesvol?		Ja/nee
Producent	Overkoepelende naam, waaronder de 'Producent' zijn producten verkoopt.	
Productnaam	Naam van het product, 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 programmatuur zoals uitgegeven door de producent

Beheer en onderhoudsdocumentatie Asset-type

Documentatie waarin met betrekking tot het betreffende Asset het volgende wordt vastgelegd :

- beheer en onderhoudsinstructies;
- vervangingsinstructies;
- handleiding CS R16 Configuratie item/Asset;
- verantwoordelijken voor het onderhoud;
- status onderhoud.
- Patch procedure

Bron: RWS CSIR

Gedocumenteerde informatie: informatie die een organisatie (2.57) moet beheren en onderhouden en het medium waarop deze informatie is vastgelegd.

Bron: NEN-ISO/IEC 27001 (nl) Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen
(ISO/IEC 27001:2017 en,IDT)

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		d-m-jjjj (let op: streepjes noodzakelijk)
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor de beheer en onderhoudsdocumentatie.
Beheer en onderhouds-documentatie Gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging van de beheer en onderhoudsdocumentatie heeft doorgevoerd.
beheer en onderhouds-instructies aanwezig?		beheer en onderhoudsinstructies: ja/nee
Vervangings-instructies aanwezig?		Vervangingsinstructies: ja/nee
handleiding CS R16 Configuratie item/Asset aanwezig?		handleiding CS R16 Configuratie item: ja/nee
verantwoordelijken voor het onderhoud aanwezig?		verantwoordelijken voor het onderhoud: ja/nee
status onderhoud bekend?		status onderhoud bekend: ja/nee
Patch procedure aanwezig?	Beschrijft de werkwijze voor het implementeren of doorvoeren van een Patch	Patch procedure: ja/nee

Data-communicatienetwerkontwerp Asset-type
Een datacommunicatienetwerk is een netwerk voor data-overdracht tussen twee of meer apparaten. De apparaten kunnen telefoons, modems, Switches, Routers, computers of onderdelen ervan zijn, maar evengoed bijvoorbeeld ook weerstations, printers, stuursystemen, mobiele telefoons, enz. De structuur waarin de apparaten door middel van het netwerk gekoppeld zijn, wordt de netwerktopologie genoemd. (Bron: https://nl.wikipedia.org/wiki/Datacommunicatienetwerk)

Het Data-communicatie-netwerk-ontwerp betreft de documentatie waarin met betrekking tot het betreffende CS Configuratie Item het volgende wordt vastgelegd :

- Fysieke topologie;
- Logische topologie;
- IP-plan; Zie de minimumeisen in de bijlage IP Plan.

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		d-m-jjjj (let op: streepjes noodzakelijk)
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor het Data-communicatie-netwerk-ontwerp.
Het Data-communicatie-netwerk-ontwerp gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging van het Data-communicatie-netwerk-ontwerp heeft doorgevoerd.
Netwerkprotocol beschrijving aanwezig?	Een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie over een communicatiemedium.	Netwerkprotocolbeschrijving: ja/nee
Fysieke topologie aanwezig?	Fysieke topologie verwijst naar het fysieke ontwerp van het netwerk. Het samenhangend geheel van elementen (o.a. routers, switches, koperdragers en glasvezels) waarover gegevens elektronische worden getransporteerd. (Bron: gebaseerd op definitie fysiek netwerk in Architectuur Netwerken en Telefonie RWS 2008-2014)	Fysieke topologie: ja/nee

Logisch topologie aanwezig?	Logische topologie verwijst naar hoe gegevens daadwerkelijk wordt overgedragen in een netwerk onafhankelijk van het fysieke ontwerp. (Bron: http://www.eecho-webdesign.com/computer-internet-technologie/network-topology/) Een voorbeeld van een logisch netwerk is het Virtual Private Network (VPN).	Logisch topologie: ja/nee
IP-plan van datacommunicatie-netwerk aanwezig?	Voor beoogde inhoud IP plan, zie de bijlage IP plan	IP-plan aanwezig: ja/nee
DNS	Domein Naam System:	

Data opslag

Onder het deelmodel Dataopslag worden de datadragers geregistreerd:

- Database
  Een database, gegevensbank of databank is een (meestal digitaal opgeslagen) gegevensverzameling, ingericht met het oog op flexibele raadpleging en gebruik. Databases spelen een belangrijke rol bij het archiveren en actueel houden van gegevens van onder meer de overheid, financiële instellingen en bedrijven, in de wetenschap, en ze worden op kleinere schaal ook privé gebruikt. (bron: Database - Wikipedia)
- Share

o Het delen van bestanden is de praktijk waarbij digitale media, zoals computerprogramma's, multimedia (audio, afbeeldingen en video), documenten of elektronische boeken worden gedistribueerd of toegang wordt verleend. Het delen van bestanden kan op een aantal manieren worden bereikt. Veelgebruikte methoden voor opslag, verzending en verspreiding zijn onder meer handmatig delen met gebruikmaking van verwijderbare media, gecentraliseerde servers op computernetwerken, op het World Wide Web gebaseerde hyperlinked documenten en het gebruik van gedistribueerde peer-to-peer netwerken. (bron: File share - Wikipedia)

We onderkennen de volgende typen Share:

i. NFS

1. is een netwerkbestandssysteem dat alle bestandssystemen op het netwerk kan delen. Als er een Windows-machine in uw netwerk is, moet u Samba gebruiken. Windows ondersteunt geen NFS; NFS, of Network File System, is een samenwerkingssysteem dat begin jaren 80 door Sun Microsystems is ontwikkeld en waarmee gebruikers bestanden op een externe computer kunnen bekijken, opslaan, bijwerken of delen alsof het een lokale computer is.

ii. Samba

1. wordt gebruikt voor het delen van linux-bestanden met Windows-netwerk ... \. De server wordt geconfigureerd om bestanden te delen met elke client op het netwerk zonder om een wachtwoord te vragen.

Database Asset-type

Veld	**Soort veld**	**Waarde / naamgeving-conventie**	**Automatische sync?**
Asset ID	Open veld	*Database naam*	Nvt (statisch)

Bron-ID (A/S-Nummer/ Leveranciers ID/Producent ID)	Open veld		
Soort	Vaste waarde	Database	Nvt (statisch)
Status	Vaste keuzes	Actief Inactief	Nee
Merk	Vaste keuzes		
Type database	Vaste keuzes	MsSQL Oracle Postgres	Nee
Specificatie *(optioneel)*	Open veld		Nee
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services OSR VM Services OSR WM Services	Nvt (statisch
Aanspreekpunt	Vaste keuzes		Nee
DBMS versie	Vaste-keuzes		Nee
OTAP-omgeving	Vaste keuzes		Nee
Capaciteit (GB)	Open veld		Nee
LCM Afvoerdatum	Datumveld		Nee
Inventarisatiedatum	Datumveld		Nee

Share Asset-type

Veld	**Soort veld**	**Waarde / naamgeving-conventie**	**Automatische sync?**
Asset ID	Open veld	SHARE-000000	Nvt (statisch)
Bron-ID (A/S-Nummer/ Leveranciers ID/Producent ID)	Open veld		
Soort	Vaste waarde	Share	Nvt (statisch)
Type Share	Vaste keuzes	NFS Samba SMB	Nee
Status	Vaste keuzes	Actief Inactief	Nee
Specificatie *(optioneel)*	Open veld		Nee
Serienummer	Open veld	Share naam-kort	Nee
Aanspreekpunt	Vaste keuzes	*TAB-team*	Nee
Eigendom	Vaste keuzes	N.v.t.	Nee
Eigenaarschap		e-mail adres verantwoordelijke Service Delivery Manager (SDM-er)	
Notities	Open veld	Share naam-lang	
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services	Nee

		OSR VM Services OSR WM Services	
OTAP omgeving	Vaste keuzes		Nee
Capaciteit (GB)	Open veld		Nee
LCM Afvoerdatum	Datumveld		Nee
Inventarisatiedatum	Datumveld		Nee

Embedded Programmatuurversie Assettype

Embedded software is computer software, written to control machines or devices that are not typically thought of as computers, commonly known as embedded systems. It is typically specialized for the particular hardware that it runs on and has time and memory constraints. Embedded programmatuur is computerprogrammatuur die is geschreven om hardware en machines te sturen die niet vallen onder wat we in het dagelijkse spraakgebruik zien als computers.
Bron: https://en.wikipedia.org/wiki/Embedded_software

Onder Embedded programmatuurversie valt bijvoorbeeld Firmware en PROGRAMMABLE LOGIC CONTROLLER (PLC).

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Attribuut	Definitie	Schrijfwijze
Object ID		Invullen door RWS
Bron ID		(Uniek ID zoals geregistreerd bij opdrachtnemer)
Soort		Keuzeveld: Firmware Overig
Status Programmatuur versie		Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Merk	Uit het Model Infra & Hardware KA: De handelsnaam, waaronder een producent een productrange op de markt plaatst.	
Hostnaam		
Mac-adres		
IP-adres		
Taal	Taalcode van de software conform ISO-693-3	Taalcode van de software conform ISO-693-3
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.
Aanschafprijs		
Sap referentie		
Aanspreekpunt invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer		
Leverancier	optioneel	
Aanschafdatum		d-m-jjjj (let op: streepjes noodzakelijk)
Installatie Datum		d-m-jjjj (let op: streepjes noodzakelijk)

EOL-End of Life datum d-m-jjjj (let op: streepjes noodzakelijk)		
EOS-End of Support datum d-m-jjjj (let op: streepjes noodzakelijk)		
Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		*Indien van toepassing*
GPS Location Lattitude		*Indien van toepassing*
GPS Location Longtitude		*Indien van toepassing*
RD X- coördinaat		*Indien van toepassin*
RD Y- coördinaat		*Indien van toepassing*
Rack (kastnummer)		*Indien van toepassing*
Rack (kasthoogte)		*Indien van toepassing*

Fysieke server Assettype
Computer die centraal taken afhandelt voor een of meer clients. De computer kan in verschillende gedaantes voorkomen: Blade, Rack mounted en Desktop.

We kennen verschillende typen servers:

- **Network DNS**: een Domain Name System (DNS) server die gebruikt wordt om namen van computers en systemen naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Bron: RWS Datamodel ServiceNow versie 1.4
- **Secure Network Server**: een Secure Network Server is een systeem dat zorgt voor geautoriseerde toegang tot verschillende netwerksystemen en applicaties. Bron: RWS Datamodel ServiceNow versie 1.4
- **Blade server**: Een server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers.Een Blade server is een computer met een modulair ontwerp dat is geoptimaliseerd om het gebruik van fysieke ruimte en energie te minimaliseren. RWS Datamodel ServiceNow versie 1.4
- **PC server**: Een server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers. Een PC server is een computer in “tower” of “rack” behuizing. RWS Datamodel ServiceNow versie 1.4
- **Server**: Een server is een fysieke computer waarop programma's draaien om diensten te verlenen aan gebruikers. Onder deze categorie vallen de overige servers waarbij geen type

behuizing wordt aangegeven, bijvoorbeeld de Moxa embedded computers. WS Datamodel ServiceNow versie 1.4.

- **ESX-Host:** Fysieke server waarop virtuele servers worden gedeployed.

Aandachtspunt: verschillende typen servers kunnen verschillende relaties hebben. Voorlopig worden ze beschouwd als verschillende Assettypes. Als vervolgstap op het model Infra en Hardware-ka versie 2.0 zal worden onderzocht in hoeverre een opschoning mogelijk is. In zijn algemeenheid geldt dat voor alle genoemde typen Server de onderstaande tabel geldt. Met als enige afwijking dat er (voorlopig nog) verschillende soortnamen en andere prefixen gelden voor de verschillende typen Servers.

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Type Server	Prefix voor Object ID	Soortnaam
Network DNS	SRVN-*	Network DNS
Secure Network Server	SRVS-*	Secure Network Server
Blade server	SRVB-*	Blade server
PC server	SRVP-*	PC server
Server	SRV-*	Server

Algemene tabel voor Server:

Veld	**Soort veld**	**Waarde / naamgevingconventie**
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Zonering		Invullen door RWS https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
MKS		Invullen door RWS
Merk	Vaste keuzes	
Type	Vaste keuzes	
Specificatie *(optioneel)*	Open veld	
Serienummer	Open veld	
Aanspreekpunt	Vaste keuzes	*Beschikbaarheid Topdesk*
Leverancier *(optioneel)*	Vaste keuzes	*Beschikbaarheid Topdesk*
Aanschafdatum	Datum veld	d-m-jjjj (let op: streepjes noodzakelijk)
Installatiedatum	Datum veld	d-m-jjjj (let op: streepjes noodzakelijk)
EOL-End of Life datum	Datum veld	d-m-jjjj (let op: streepjes noodzakelijk)
EOS-End of Support datum	Datum veld	d-m-jjjj (let op: streepjes noodzakelijk)
Status	Vaste keuzes	Voorraad Gereserveerd Actief Tijdelijke opslag Vermist Onderhoud

		Af te voeren Uit beheer Gedeactiveerd
Plaatskoppeling *(optioneel)*	Opzoekveld	Dropdownlijst (optioneel: indien beschikbaar gesteld door RWS)
Hostnaam	Open veld	
IP-adres	Open veld	
Beoogd gebruik	Vaste keuzes	Invullen door RWS Keuze mogelijkheden: - <u>Standaard:</u> ➔ extra keuzeveld: KA-vrij Niet-vrij. - <u>Productie:</u> Extra vrije tekstveld: waarin gegevens voor een koppeling naar de Services en een nadere sub verdeling over gebruik en/of applicatie kan worden in gevuld.
Eigenaarschap (Service Delivery Manager)	Opzoekveld	(service Delivery Manager) invullen door RWS dynamische dropdownlijst die refereert aan de persoonstabeltabel.
IP-adres *(optioneel)*	Open veld	
Hostnaam	Open veld	
IP Adres iLO *(Optioneel)*	Open veld	
OS Beheerder	Vaste keuzes	*invullen afhankelijk van contractuele afspraken:*
Operating System	Vaste keuzes	
SAP Referentie	Open veld	
Projectnummer	Open veld	
Aanschafprijs	Open veld	
Aantekeningen	Open veld	
Vestiging	Opzoekveld	Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer	Opzoekveld	Locatie opzoeken in dropdownlijst met locaties in Topdesk Indien van toepassing
GPS Location Lattitude	nummeriek	Indien van toepassing
GPS Location Longtitude	nummeriek	Indien van toepassing
RD X-coördinaat	tekst	Indien van toepassing
RD Y-coördinaat	tekst	Indien van toepassing
Rack		

kast(nummer)		
Rack Kast(hoogte)		

Hardware Asset-type

Hieronder volgt een overzicht van de attribuuttypes die in zijn algemeenheid gelden voor Hardware assets.
Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder Hardware vallen (bijvoorbeeld de definities e.d.): raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld. De inhoud is reeds opgenomen in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.

Object ID:	Unieke identificatiecode van het asset in de CMDB van Topdesk
Bron ID	Unieke identificatiecode van het asset in de brondatabase. Bijvoorbeeld van de opdrachtnemer of de regionale dienst.
Zonering	Alleen van toepassing op de Fysieke en Virtuele server. Invullen door RWS, zie: https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
Soort:	Functionaliteit van het item / Assettype. Zie voor de types het Tabblad Model Infra en Hardware KA in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.
Merk:	Merk van het betreffende item
Type:	Typebeschrijving die volgens de producent wordt gehanteerd.
Specificatie:	Open veld waar extra informatie over het item.
Serienummer:	Serienummer van het betreffende item. Vaak te achterhalen op de kast van het apparaat.
Aanspreekpunt:	Verantwoordelijke beheergroep (dropdownlijst behandelaarsgroep in Topdesk)
Leverancier:	Leverende partij, doorgaans een externe partij.
Aanschafdatum:	Leverdatum van het item. Datum staat op de pakbon genoteerd welke bij de levering wordt meegestuurd.
Installatie Datum:	
EOL End of life datum	Wordt gecommuniceerd door de leverancier,
EOS-End of support datum	Wordt gecommuniceerd door de leverancier, is een waarschuwing voor de EOL (zie boven). De leverancier biedt geen ondersteuning meer voor het betreffende item.
Status:	Geeft aan in welke toestand het item zich bevindt.
Voorraad	Item is beschikbaar voor inzet en bevindt zich doorgaans in een (de)centrale voorraad ruimte of magazijn.
Actief	Item is ingezet in de operatie en is onderdeel van de operationele keten.
Tijdelijke opslag	Item is tijdens een verbouwing of verhuizing van een kantoor tijdelijk opgeslagen.
Vermist	Item bevindt zich niet op de aangegeven locatie en is ook niet meer traceerbaar.
Onderhoud	Er wordt onderhoud gepleegd op het item. Status onderhoud is ook toepasbaar bij reparatie.
Af te voeren	Item is “End of Life” en kan daarom worden afgevoerd. De status is ook toepasbaar indien het item niet meer kan worden gerepareerd.
Uit beheer	Item is actief en aangesloten aan het netwerk maar wordt niet beheerd. Dit aangezien het item op dat moment geen deel uitmaakt van een dienst.
Gedeactiveerd	Item staat niet op voorraad, bevindt zich doorgaans in een server rack en kan aangesloten zijn met netwerkkabels en netsnoer. Het items is echter niet ingeschakeld en is dus gedeactiveerd.

Gereserveerd	Betreffende hardware is al ingericht voor een specifieke aanvrager maar nog niet in gebruik (het betreft meestal laptops)
Hostnaam:	Betreft de FQDN, het unieke adres van een computer op het RWS netwerk in de vorm van letters.
IP-adres:	Het unieke adres van een computer op het RWS netwerk in de vorm van cijfers. Dit betreft het zogenaamde Productie IP-adres waaraan ook de Hostnaam (FQDN) is gekoppeld.
Beoogd gebruik:	Geeft de beoogde gebruiksvorm aan van het item: Keuze mogelijkheden: - <u>Standaard:</u> Bij de keuze van "Standaard" hoort een extra keuze (veld) met de waarden "KA-vrij" en "Niet-vrij". - <u>Productie:</u> Bij de keuze Productie hoort de mogelijkheid voor vrije tekst (een extra vrijetekst veld) waarin gegevens voor een koppeling naar de Services en een nadere sub verdeling over gebruik en/of applicatie kan worden ingevuld.

Toelichting begrippen Standaard en Productie:

'Standaard'
Definitie '*Geautomatiseerde werkplek zoals die aan iedere medewerker van Rijkswaterstaat beschikbaar wordt gesteld. Deze werkplek wordt gedefinieerd volgens de standaarden en requirements van KA-services.*';
'Productie'
Definitie '*Geautomatiseerde werkplek met afwijkende standaarden en/of requirements ten opzichte van de standaarden en requirements zoals die door KA-services zijn gedefinieerd voor de Standaard werkplek.*'

Eigenaarschap (Service Delivery Manager): dynamische dropdownlijst die refereert aan de persoonstabeltabel.

OS-beheerder	Beheergroep van de Operating System (Wie voert OS patches uit?)
Operating system	Operarating system van de server

SAP Referentie:	Referentie welke ook in het SAP systeem van RWS wordt herkend
Aanschafprijs:	
Projectnummer:	
Levert aan/Ouder-Kind relatie:	Zie de toelichting in hoofdstuk 2
Aantekeningen:	Losse aantekeningen die relevant zijn voor het beheer.
Vestiging Topdesk	Indien van toepassing: Vestigingen opzoeken in dropdownlijst in
Overige plaatsbepaling zoals kamernummer locaties in Topdesk	Indien van toepassing: Locatie opzoeken in dropdownlijst met
GPS Location Lattitude	Indien van toepassing
GPS Location Longtitude	Indien van toepassing
RD X- coördinaat	Indien van toepassing
RD Y- coördinaat	Indien van toepassing
Ruimte	Indien van toepassing
Rack (kast) nummer	Indien van toepassing
Rack (kast) hoogte	Indien van toepassing

IV Service

Definitie Service:
Een afgebakende prestatie van een persoon of organisatie, die voorziet in een behoefte van haar afnemers.

Kenmerken:
- Een service levert meestal één of meerdere assets als producten of beheert één of meerdere assets als beheerde objecten.
- Een service kan samengesteld zijn.
- Als een service een product levert, is het gespecificeerd welk product of producten het zijn en onder welke condities ze geleverd worden.
- Als een service een asset beheert, is het gespecificeerd welk asset of assets het zijn en onder welke condities ze worden beheerd. Denk bijvoorbeeld aan service levels.
- Afbakening van de prestatie wordt bepaald door de afspraken met de (interne en/of externe) afnemers, functionele beschrijvingen en andere afspraken over het wat en hoe te leveren of beheren.
- Een service heeft een integrale TCO (Total Costs of Ownership) - alle kosten gerelateerd aan de aanschaf en gebruik gedurende de levenscyclus van ingekochte goederen en diensten. Deze kosten worden vertaald naar kostprijsmodel.

NB: alleen de witte velden dienen door de opdrachtnemer te worden ingevuld.

Veld	**Soort veld**	**Waarde / naamgevingconventie**	**Topdesk implementatie**
Asset ID	tekst	Unieke IDnaam van de Service . Start met een punt. Topdesk accepteert geen dubbelingen Krijgt de naam van de instantie. Bijv:	Omdat dit op de hoofdkaart alleen maar gekoppeld kan worden
Entity ID	Database ID:tekst? Nog uitzoeken	De tool (Topdesk) zelf automatisch een nummer laten aanmaken	
Bron ID (S-nummer/KPN/Expertdesk) invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	tekst	In overleg met RWS eigen Bron ID van de opdrachtnemer of: Productlijn ID (s nummer) Of Expertdesk ID Of KPN ID	
IV Servicegroep/Categorie	Opzoekveld	Keuzewaarden: AOA services BOS services IVP Tooling VM Services	Verplicht in Topdesk

		SVM Services IRI connectivitservices (hieronder valt KPN)	
IV Servicenaam/Subcategorie	tekst		Verplicht in Topdesk
IV Service versie	tekst		
Status IV Service	Opzoekveld	Gepland Verkrijgen of bouwen Ontwikkeling en transitie Geleverd en ondersteund End of Service Statussen conform ITIL	Verplicht in Topdesk
OTAP Omgeving	Opzoekveld	Productie (default) Acceptatie Test Ontwikkeling Training	Verplicht in Topdesk
Servicemanager	Opzoekveld	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Service Delivery Manager	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Applicatie-Product-Platformmanager invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	idem	Applicatie-Product-Platformmanager of soortgelijke manager op hetzelfde praktische niveau. Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	verplicht
Functioneel Beheerder invullen afhankelijk van contractuele afspraken: RWS of Opdrachtnemer	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	Niet verplicht
Informatiemanager	idem	Dit veld geeft een opzoeklijst met alle in TOPdesk bestaande personen.	Niet verplicht
Externe partij (leverancier en/of beheerder)		Externe partij met wie de CIV direct contact heeft.	
Vestiging	Opzoekveld		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing

Overige plaatsbepaling zoals kamernummer	Opzoekveld		Locatie opzoeken in dropdownlijst met locaties in Topdesk Indien van toepassing
GPS Location Lattitude	nummeriek		Indien van toepassing
GPS Location Longtitude	nummeriek		Indien van toepassing
RD X- coördinaat	tekst		Indien van toepassing
RD Y- coördinaat	tekst		Indien van toepassing
Contractsoort Klantcontract		Vaste keuzes (verplicht)	Keuzes: -SLA = afspraak met de eindklant -Niet van toepassing want het betreft een CIV-levering.
Contractsoort Leveranciercontract		Vaste keuzes (verplicht)	OLA = afspraak tussen CIV- afdelingen. Underpinning contract = afspraak tussen CIV afdelingen met leveranciers/externe opdrachtnemers zoals KPN.

Locatie

Definitie locatie

Vanuit het OTL wordt de volgende definitie beschikbaar gesteld:
A composite element that is a conceptual or physical place or position where concepts are located (e.g., structure elements) or performed (e.g., behavior elements).
Bron: De Werkwijzer RWS. Deze bevat de ABDL: algemene begrippen en definitie lijst.

Vanuit configuratiemanagement is er behoeft aan een meer gedetailleerde definitie en attribuuttype. Daarom gebruiken we de volgende omschrijving (goedgekeurd door het ICMO en de IGA data architecte):
In de geografie is de locatie een positie of punt in de ruimte, uitgedrukt relatief ten opzichte van een ander punt of ding. Een absolute locatie kan vaak worden gedefinieerd met behulp van cartesiaanse coördinaten, zoals gebruikmaking van specifieke breedtegraad en lengtegraad. Op Aarde kunnen de geografische coördinaten worden gebruikt om de locatie van een positie te specificeren.
Een locatie kan behalve absoluut – de exacte locatie van iets of iemand – ook relatief zijn, de positie van iemand ten opzichte van iets anders.

Bron: https://nl.wikipedia.org/wiki/Locatie

Opmerking: het is in de huidige CMDB van RWS nog niet mogelijk om Locatietabellen toe te voegen. Daarom zullen we **voorlopig** werken met het toevoegen van **Locatie-eigenschappen** aan de **attribuutvelden van de CI-items/Assets**. Zie hiervoor de attribuuttypes bij de uitgewerkte Asset.

Zie onder voor de Locatietabel

Locatie Tabel

Algemene business rule: alles wat van toepassing is, invullen. Wanneer de asset zich binnen een bekende vestiging bevindt, zijn coördinaten niet nodig.

Attribuut	Definitie	Schrijfwijze	Bron
		Generiek	
UI	Unieke identificatiecode		idem
GPS Longitude		Volgens GPS format	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
GPS Latitude		Volgens GPS format	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
RD x-coördinaat		Volgens Rijksdriehoek	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
RD y-coördinaat		Volgens Rijksdriehoek	Zo nauwkeurig als mogelijk, minimaal op vierkante meter nauwkeurig.
		Specifiek	
BAG ID Indien het een BAG pand betreft, anders naar overig			ID zoals in de BAG geregistreerd.
IV locatie buiten ID			Bijv. KPN Voor infra buiten.
VM locatie ID			
SVM locatie ID			
WM locatie ID			
Asset Management locatie ID			
Vestiging			NU: Vestigingen opzoeken in dropdownlijst in Topdesk
Overige Plaatsbepaling zoals kamernummer			Locatie opzoeken in dropdownlijst met locaties in Topdesk.
Ruimte			
Rack (kast)nummer			
Rack (kast)hoogte			

Licentie Asset-type

Het recht op het gebruik van software/programmatuur en hardware

Bron: RWS CSIR

NB: dit Assettype is nog onder constructie. Voor de meest actuele versie en meer informatie over dit Asset-type: raadpleeg het model Programmatuur, deze zal op aanvraag beschikbaar worden gesteld

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer

Bestelnummer	Conform SAP. Niet elke licentie kent een BESTELNUMMER, alleen die, die niet onder een contract hangen. Ook wel ‘4500‘ genoemd.	Conform SAP. Niet uniek.
Onderhouds-contract	Het contract houdt in, dat de betreffende items door de leverancier in optimale conditie wordt gehouden.	‘Ja‘ of ‘Nee‘.
Supportcontract	Het contract houdt in, dat de leverancier dienstverlening uitvoert ten behoeve van de afnemer.	‘Ja‘ of ‘Nee‘.
Licentiecontract	Het contract houdt in, dat de levancier de afnemer het recht geeft gebruik te maken van het gelicenceerde goed.	‘Ja‘ of ‘Nee‘.
Soort licentie	Het soort licentie dat is afgesloten, Proprietary, Open Source of geen (PD)	Het soort licentie dat is afgesloten, Proprietary, Open Source of geen (PD)
Berekeningsbasis gebruiker	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Berekeningsbasis installatie	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Berekeningsbasis gebruik	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.	De wijze waarop de fee berekend wordt, die men verschuldigd is als gevolg van het aanvaarden van de licentie.
Aantal	Het aantal legale, ingekochte licenties van deze soort en berekeningswijze.	Positief geheel getal.

Bron tabel: Conceptueel Datamodel Configuratie Management versie 1.0 vastgesteld.

Programmatuurbeschrijving Asset-type

Documentatie waarin met betrekking tot het betreffende CS R16 Configuratie Item -> Programmatuur Item het volgende wordt vastgelegd :

- Programmeertaal
- Communicatieprotocol (laag 7 van het OSI model), bijvoorbeeld:
  - LDAPversie
  - SMTPversie
  - HTTPversie

Bron: RWS CSIR

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Plaats	Waar kan de beheerdocumentatie worden gevonden?	Dit kan zowel een digitaal als fysiek adres zijn. Zo specifiek mogelijk dus indien van toepassing ook kamernummer en kast vermelden.
Datum laatst gewijzigd		ISO 8601 formaat: jjjj-mm-dd
Verantwoordelijk		Naam, organisatie en contactgegevens van de persoon die verantwoordelijk is voor de Programmatuurbeschrijving.
Programmatuur beschrijving Gewijzigd door?		Naam, organisatie en contactgegevens van de persoon die de laatste wijziging in de Programmatuurbeschrijving heeft doorgevoerd.
Aanleiding wijziging	Referentie aan Changeproces	
Programmeertaal		
Communicatie-protocol	Transportlaag (Laag 4) OSI model. (zie bijlage)	Keuzelijst: TCP, UDP of ISO-on-TCP(rfc1006) en het poortnummer (bv 80, 443, 22 etc).
Patch toegepast	Sprake van een Patch: ja/nee	
Datum laatste Patch		d-m-jjjj (let op: streepjes noodzakelijk)

Programmatuurversie Asset-type

De (door Opdrachtnemer op te leveren) set programmaregels zoals die, op directe of indirecte wijze, door een computer kan worden gebruikt om een bepaald, nader omschreven, resultaat tot stand te brengen. Programmatuur kan worden onderscheiden in Standaard- en Maatwerkprogrammatuur

Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur
Artikel 1: Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur, 2n.

Voor de meest actuele versie en meer informatie over de soorten/Asset-types die onder het Data model Programmatuur vallen (bijvoorbeeld de definities e.d.): raadpleeg het Data model Programmatuur, deze zal op aanvraag beschikbaar worden gesteld. De inhoud is reeds opgenomen in de bijgeleverde CMDB Cybersecurity Industriële Automatisering Excel Format.

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Status Programmatuur versie	Keuzeveld	Keuzeveld: Ge-Deïnstalleerd Geïnstalleerd Niet geïnstalleerd Ontwikkelen
Missie Kritieke Systemen (MKS)	Het Programmatuur item is onderdeel van één of meer door Rijkswaterstaat vastgestelde Missie Kritieke Systemen. Deze informatie moet door Rijkswaterstaat worden aangeleverd.	Invullen door RWS Opsomming van de MKS(en) waarvan het Programmatuur item deel uitmaakt. Schrijfwijze zoals gehanteerd in lijst vastgestelde MKS.
Versie	Een specifieke variatie of verdere ontwikkeling van een origineel product	Zonder voorloop-V, nummers gescheiden door punten.
Programmatuur-type	Het soort applicatie/programmatuur, dat het hier betreft conform de indeling 'applicatietype'.	Keuzelijst: standalone applicatie, webapplicatie, client applicatie, mobile app, plug-in, clouddienst (SAAS), serverapplicatie (backend), Operating System
Producent	Overkoepelende naam, waaronder de 'Producent' zijn product verkoopt.	
Productnaam		Naam van de programmatuur zoals uitgegeven door de producent
Ordenummer Vendor		
Taal [ISO-639-3]		ISO codes (2 karakters): NL, DU, EN, etc.
Maatwerktype	In hoeverre er hier sprake is van maatwerk en welk type maatwerk het betreft.	Keuzelijst: keuzelijst: COTS, MOTS (modified of the shelf), maatwerk
A/B/C klassificatie	[A] Applicaties/Programmatuur die standaard worden geleverd op de standaard Werkstation. [B] Applicaties/Programmatuur die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig. Vastgesteld door RWS-bestuur.	Keuzelijst: [A] Applicaties die standaard worden geleverd op de standaard Werkstation. [B] Applicaties die optioneel door iedere Werkplekgebruiker kunnen worden aangevraagd. [C] Overig.

Vestiging		Vestigingen opzoeken in dropdownlijst in Topdesk Indien van toepassing Let op: vaak niet beschikbaar voor opdrachtnemer dan als alternatief de adresgegevens invullen. Zie Excel
Overige plaatsbepaling zoals kamernummer		
GPS Location Lattitude		
GPS Location Longtitude		
RD X- coördinaat		
RD Y- coördinaat		

Virtueel Cluster Asettype

Indien van toepassing: Raadpleeg het model Infra & Hardware- KA, deze zal op aanvraag beschikbaar worden gesteld.

Virtuele server Asset-type

Virtualisatie maakt het mogelijk om op een fysieke server een (groot) aantal virtuele servers te gebruiken waardoor de fysieke server een veel groter deel van de tijd gebruikt wordt.
Bron: https://nl.wikipedia.org/wiki/Virtual_private_server

Raadpleeg voor de meest actuele versie ook het model Infa & Hardware-KA, deze zal op aanvraag beschikbaar worden gesteld.

Veld	**Soort veld**	**Waarde / naamgeving-conventie**
Object ID	Open veld	Invullen door RWS VM naam van virtuele server
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Zonering		Invullen door RWS https://www.noraonline.nl/wiki/Beschouwingsmodel_zonering
Soort	Vaste waarde	Virtuele Server
Merk	Vaste keuzes	Windows Linux
Type	Vaste keuzes	Algemeen Applicatieserver (shared) Databaseserver Licentieserver Loadbalancer Webserver

		Servercapaciteit Werkstation ….
Specificatie (optioneel)	Open veld	
Serienummer (optioneel)	Open veld	(Oude VM-nummer van vóór de migratie)
Installatie door	Vaste keuzes	
Aanspreekpunt	Vaste keuzes	
Plaatskoppeling	Vaste waarde	Configuratie
Configuratie ID	Vaste keuzes	*Beschikbaarheid Topdesk*
Status	Vaste keuzes	o.a.: Actief Inactief
Aantal CPU'	Open veld	
RAM Geheugen	Open veld	GB, afgerond naar 1 decimaal
Toegekend schijfruimte	Open veld	Afgerond naar hele GB's
Productdomein	Vaste keuzes	IRN BV Ontwikkeling en Services IRN IV Infrastructuur IRN IV Platformen OSR A en O Services OSR SVM Services OSR VM Services OSR WM Services
Primair product	Open veld	
OTAP(L) omgeving	Vaste keuzes	Ontwikkel Test Acceptatie Productie Les
Infra service / bouwsteen		
Serienummer	Open veld	(het UUID van de VM volgens VMWare)
Hostnaam	Open veld	
IP-adres (optioneel)	Open veld	
OS Beheerder		
Eigenaarschap (Service Delivery Manager)		dynamische dropdownlijst die refereert aan de persoonstabeltabel.
Operating System	Open veld	
LCM Afvoerdatum	Datum veld	d-m-jjjj (let op: streepjes noodzakelijk)

Wijzigingendocument (Escrow) Asset-type

Soorten:
- Escrow
- Overig

Toelichting Escrow:

Het deponeren van (een kopie van) de Broncode van Standaardprogrammatuur waarin aanpassingen zijn gedaan specifiek ten behoeve van Opdrachtgever bij een onafhankelijke derde opdat Opdrachtgever deze, bij het in vervulling gaan van een of meer in de Escrow overeenkomst bepaalde voorwaarden, eigenmachtig kan (laten) gebruiken voor het herstellen van fouten en anderszins onderhouden, verder ontwikkelen en beheren van de Standaardprogrammatuur.

Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur
Artikel 1: Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur, 2d.

Escrow omvat alle niet openbaargemaakte informatie die de Opdrachtgever redelijkerwijs nodig heeft voor foutherstel, onderhoud, verder ontwikkelen en beheer van de Standaardprogrammatuur zodat hij daarvan het overeengekomen gebruik kan blijven maken. Escrow voldoet aan het geen dienaangaande ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is.
COTS Programmatuur valt buiten de scope van Escrow

Zie ook Bron: Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur Artikel 7:Escrow, bijlage A voor de eisen die aan Escrow worden gesteld.

Attribuut	Definitie	Schrijfwijze
Object ID	Open veld	Invullen door RWS
Bron ID		Uniek ID zoals geregistreerd bij opdrachtnemer
Escrow documentatie aanwezig?	Keuzeveld	Ja nee
Datum eerste deponering	Datum waarop de eerste deponering van de Escrow heeft plaatsgevonden	d-m-jjjj (let op: streepjes noodzakelijk)
Datum laatste deponering	Datum waarop de eerste deponering van de Escrow heeft plaatsgevonden	d-m-jjjj (let op: streepjes noodzakelijk)
Escrow agent	De in te zetten Escrow agent heeft expertise om het gedeponeerde Product en bijbehorende Materialen te controleren op aanwezigheid, volledigheid en bruikbaarheid. Het Product en bijbehorende Materialen	Naam, organisatie en contactgegevens van de Escrow agent.

De CMDB opbouw en onderhoud dient conform de CMDB Cybersecurity Industriële Automatisering Excel Format vorm gegeven te worden. De Excel Format is op verzoek verkrijgbaar bij het Security Centre van CIV.

CMDB
Cybersecurity Indust

Bijlage CSR 17 Beveiligingshuisregels

CSR 17.1 Doelstelling

Aanvallen van buitenaf, malware en andere security incidenten kunnen ervoor zorgen dat er schade ontstaat aan een object of de industriële automatisering die het object bestuurt. Opdrachtnemer dient daarom huisregels te hebben voor het werken binnen en met IA-omgevingen. Deze huisregels helpen bij het op een verantwoorde en cyberveilige manier te werken. Net als bij de persoonlijke veiligheid geldt: we werken veilig of we werken niet.

CSR 17.2 Best practices

De beveiligingshuisregels dienen kenbaar te worden gemaakt aan alle vaste medewerkers op het object en te worden verstrekt aan alle bezoekers aan het object. Hierbij dienen duidelijk naam en telefoonnummer van de objectbeheerder en het telefoonnummer voor storingsmeldingen te worden vermeld.

De beveiliging van bedienbare objecten, verkeersposten en bediencentrales is een verantwoordelijkheid van ons allemaal. Van beheerder, monteur tot bedienaar: samen helpen we misbruik en fouten te voorkomen.

De beveiligingshuisregels bevatten ten minste het volgende:

a. Toegang tot deze locatie is alleen toegestaan voor wie zich heeft aangemeld bij de objectbeheerder;
b. Meld het vermoeden van een beveiligingsincident net zoals andere storingen. Geef bij de melding aan dat het (mogelijk) om een beveiligingsincident gaat. Voorbeelden zijn virusbesmetting, plotseling en onverklaarbaar verlies van zicht op of controle over het object, een verloren USB-stick/laptop, het object komt plotseling in beweging zonder dat hiervoor opdracht is gegeven door de bedienaar;
c. Loopt er iemand op het object die je niet kent? Ga na of deze persoon op het object hoort te zijn en of deze persoon toegang mag hebben tot de IA apparatuur;
d. Wijzig systemen alleen met toestemming van de objectbeheerder. Meld je bij werkzaamheden aan en af bij de objecteigenaar. Zorg voor een werkvergunning als deze nodig is voor de werkzaamheden;
e. Het is voor gebruikers niet toegestaan zelf software te installeren;
f. Leen passen en sleutels niet uit zonder toestemming van de objectbeheerder. Persoonlijke accounts en wachtwoorden deel je nooit met anderen, ook niet met collega’s;
g. Voorkom dat informatie in verkeerde handen kan vallen. Bij twijfel over het delen van informatie, raadpleeg de objectbeheerder vóórdat informatie wordt gedeeld;
h. Sla wachtwoorden beveiligd en niet zichtbaar voor anderen op. Gebruik hiervoor een elektronische wachtwoordkluis;
i. Mobiele apparatuur mag niet onbeheerd worden achtergelaten;
j. Sluit bij onderhoudswerkzaamheden alleen USB-sticks of apparaten aan die op malware zijn gescand. Scan de aangesloten apparatuur ook achteraf nogmaals op malware. Sluit nooit persoonlijke apparatuur zoals telefoons aan op de IA-omgeving;
k. Sluit (internet)verbindingen (wifi, 4G, 5G, Bluetooth, etc) af op apparatuur die wordt aangesloten op de IA-omgeving, vóórdat de apparatuur gekoppeld wordt. Sluit geen draadloze netwerken aan op de IA-omgeving;
l. Creëer geen eigen netwerken en koppelingen. Alleen een RWS-netwerk mag gebruikt worden voor externe verbindingen;
m. Log systemen uit na gebruik op en ruim apparatuur op (netwerkkabels, USB-sticks, externe harde schijven, etc);
n. Haal na gebruik de sleutel uit het slot of de schakelaar. Berg sleutels veilig op;
o. Sluit deuren en ramen af en doe ze op slot. Doe serverkasten en werkruimtes op slot als je er niet bezig bent en altijd als je weg gaat;
p. Spreek elkaar aan op het niet naleven van deze regels.

Bijlage CSR 18 Back-up en recovery

CSR 18.1 Doelstelling

Door apparatuur die kapot gaat, een security incident, of andere oorzaak, is het mogelijk dat een back-up moet worden teruggezet. Het is dan van belang dat er een actuele, werkende back-up is. Een goede back-up strategie zorgt ervoor dat het back-up proces voorspoedig verloopt met een minimale impact op de operationele status van het object.

CSR 18.2 Best practices

Een goede back-up strategie voorziet tenminste in het volgende:

a. Bepaal van welke systemen op het object back-ups gemaakt dienen te worden;
b. Zorg dat de benodigde materialen aanwezig zijn;
c. Maak voor elk systeem een duidelijk stappenplan voor het maken van de back-ups, toegepast op de specifieke situatie;
d. Maak voor elk systeem een duidelijk stappenplan voor het terugzetten van de back-ups, toegepast op de specifieke situatie;
e. Maak back-ups van elk systeem;
f. Controleer of de gemaakte back-ups de informatie bevatten die nodig is voor een succesvolle restore en of deze correct functioneren;
g. Sla de back-ups op, zowel on-site als off-site;
h. Bij wijzigingen aan een systeem, maak een nieuwe back-up;
i. Controleer de back-up's jaarlijks middels een recovery test.

Benodigde materialen

Verschillende materialen kunnen benodigd zijn voor het maken en controleren van back-ups. Voorbeelden hiervan zijn:

a. Sleutel voor het openen van de serverkast / besturingskast;
b. Versleutelde harde schijf;
c. Back-up software;
d. Toetsenbord en muis;
e. Externe DVD-ROM drive en DVD-ROM's;
f. Inloggegevens van de systemen waarvan een back-up gemaakt wordt;
g. Werkvergunning.

Bijlage CSR 19 Intellectueel eigendom

CSR 19.1 Doelstelling

RWS maakt gebruik van bedrijf kritische Programmatuur ter aansturing of ondersteuning van de maatschappelijk vitale processen. Daarmee ontstaat afhankelijkheid van de leveranciers, die deze Programmatuur (op maat) ontwikkelden en/of moeten onderhouden. Het staken van de bedrijfsactiviteiten of het failliet gaan van de leverancier introduceert serieuze risico's voor de continuïteit van de maatschappelijk vitale processen van RWS. Om deze continuïteitsrisico's te mitigeren moet RWS in de contracten goede afspraken maken over de Intellectuele Eigendomsrechten van Maatwerk Programmatuur en/of een Escrow overeenkomst aangaan voor Standaardprogrammatuur waarvan de intellectuele eigendomsrechten bij Opdrachtnemer of derden liggen.

Intellectueel Eigendom

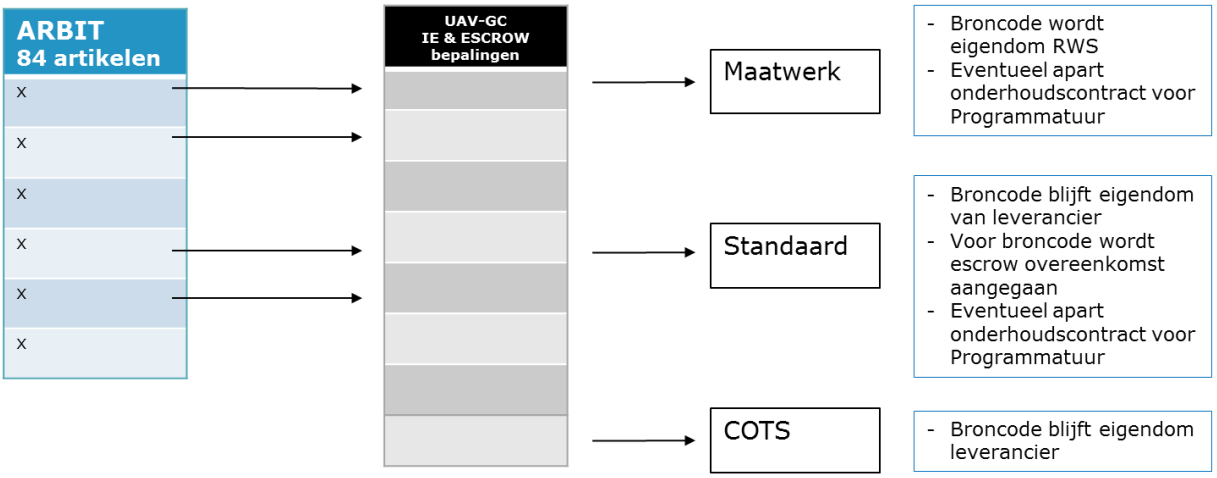
Intellectueel Eigendomsrechten zijn exclusieve rechten van rechthebbenden op een voortbrengsel van de menselijke geest. Een voorbeeld daarvan is het auteursrecht, waar Programmatuur onder valt. IE-rechten stellen de eigenaar in staat het werk (Programmatuur) te exploiteren.

Inkoopvoorwaarden

RWS maakt gebruik van de Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT). De ARBIT bestaat uit algemene- en bijzondere bepalingen die betrekking hebben op alle IT-overeenkomsten die de Opdrachtgever aangaat en bevat 84 artikelen die de verhouding tussen de overheid als Opdrachtgever en ICT-bedrijven als leverancier vastleggen. Een aantal van deze artikelen gaat over het Intellectueel Eigendom van Programmatuur en beschrijft wanneer een Escrow overeenkomst moet worden aangegaan tussen Opdrachtgever en Opdrachtnemer.

Echter voor de uitvoering van werken en van technische installatiewerken maakt RWS gebruik van de Uniforme Administratieve Voorwaarden Geïntegreerde Contractvormen (UAV-GC). Deze voorwaarden zijn een combinatie van inkoop- en leveringsvoorwaarden. *D*e UAV-GC bevat onvoldoende bepalingen voor Intellectueel Eigendom en Escrow van Programmatuur om de continuïteit van de primaire en ondersteunende systemen binnen de Infrastructuur van RWS te waarborgen in geval van staken, overname of failliet gaan van een leverancier. RWS heeft dan ook een "Bijlage bijzondere bepalingen IA gerelateerde Programmatuur" ontwikkeld om in deze leemte van de UAV-GC te voorzien. Hierbij is gebruik gemaakt van de artikelen uit de ARBIT-2018 die het Intellectueel Eigendom en Escrow tussen Opdrachtgever en Opdrachtnemer regelen. Waar mogelijk is de tekst van de artikelen en de definities van de begrippen uit de ARBIT integraal aangehouden. Om inconsistenties tussen de ARBIT en UAV-GC bepalingen en begrippen te voorkomen zijn enkele artikelen en begrippen aangepast en/of toegevoegd.

In de volgende afbeelding wordt de mapping van de relevante artikelen uit de ARBIT-2018 naar toepassing binnen de UAV-GC weergegeven. Ook wordt op hoofdlijnen aangegeven in welke situatie er een overdracht van de broncode plaatsvindt van de Opdrachtnemer naar Opdrachtgever of dat er een Escrow overeenkomst moet worden aangegaan.



CSR 19.2 Bijzondere bepalingen Industriële Automatisering gerelateerde Programmatuur

Artikel 1 Begripsbepalingen Industriële Automatisering gerelateerde Programmatuur

1. Deze bijzondere bepalingen gelden alleen voor Programmatuur gerelateerd aan Industriële Automatisering.
2. Aan de volgende in deze bijzondere bepalingen met een hoofdletter gebezigde woorden wordt, aanvullend op de gedefinieerde begrippen in paragraaf 1 UAV-GC, de bijbehorende betekenis toegekend:

    a. Broncode: De Programmatuur en het geheel van programma-instructies in de oorspronkelijke programmeertaal met inbegrip van de daarbij behorende Documentatie in een zodanige vorm dat een programmeur die beschikt over kennis en ervaring van de gebruikte programmeerwijze en techniek, daarmee de Programmatuur kan wijzigen.

    b. Commercial Off-The-Shelf (COTS): De programmatuur welke commercieel ter beschikking wordt gesteld (geleased, gelicentieerd of verkocht) aan de markt, welke geen speciale aanpassing of onderhoud vereist gedurende de levensduur. Het intellectueel eigendom ligt bij de producent.

    c. Documentatie: Iedere beschrijving van Broncode, Objectcode, het Product en de eigenschappen daarvan bestemd voor de installatie, implementatie, het gebruik, beheer en/of het onderhoud daarvan alsmede de beschrijving van alle hulpmiddelen zoals systeemvereisten voor de ontwikkelomgeving met bijbehorende configuratie en instellingen en de stappen om van Broncode tot Objectcode te komen.

    d. Escrow: Het deponeren van (een kopie van) de Broncode van Standaardprogrammatuur waarvan het intellectueel eigendom bij de Opdrachtnemer ligt en waarin aanpassingen zijn gedaan specifiek ten behoeve van Opdrachtgever bij een onafhankelijke derde opdat Opdrachtgever deze, bij het in vervulling gaan van een of meer in de Escrow overeenkomst bepaalde voorwaarden, eigenmachtig kan (laten) gebruiken voor het herstellen van fouten en anderszins onderhouden, verder ontwikkelen en beheren van de Standaardprogrammatuur.

    e. Gebrek: Een gebrek conform paragraaf 4.1 UAV-GC dat in het kader van deze bijlage mede omvat iedere storing en/of mankement als gevolg waarvan de Prestatie niet geschikt is voor het overeengekomen gebruik.

f. Gebruiksrecht: Het recht op grond waarvan de Opdrachtgever bevoegd is tot het installeren en gebruiken van Standaardprogrammatuur overeenkomstig het overeengekomen gebruik conform de bepalingen van deze Overeenkomst met inbegrip van alle daarvoor redelijkerwijs noodzakelijke al dan niet tijdelijke verveelvoudigingen.

g. Industriële Automatisering (IA): 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.). Het voorgaande omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen).

h. Installatiekopie: Een gegevensdrager met daarop de Standaardprogrammatuur waarvoor het Gebruiksrecht wordt verleend.

i. Maatwerkprogrammatuur: Specifiek ten behoeve van de Opdrachtgever te ontwikkelen of ontwikkelde Programmatuur. Het intellectueel eigendom ligt bij de Opdrachtgever.

j. Materialen: Voor installatie, implementatie, gebruik en/of beheer en onderhoud van het Product benodigde hulpmiddelen, zoals de ontwikkelomgeving inclusief de hardware en software waaronder conversiesoftware, kabels, smartcards en fysieke gegevensdragers waarop Programmatuur wordt geleverd.

k. Objectcode: Vertaling van de Broncode in een direct door een computer leesbare en uitvoerbare code.

l. Patch: Als tijdelijk bedoelde correctie van Programmatuur.

m. Product: de Broncode, de Objectcode, de Programmatuur, de Documentatie en bijbehorende Materialen, inclusief alle aanpassingen van deze productonderdelen.

n. Programmatuur: De door Opdrachtnemer op te leveren set programmaregels zoals die, op directe of indirecte wijze, door een apparaat kan worden gebruikt om een bepaald, nader omschreven, resultaat tot stand te brengen. Programmatuur kan worden onderscheiden in Standaard- en Maatwerkprogrammatuur.

o. Standaardprogrammatuur: Voor algemeen gebruik ontwikkelde Programmatuur van de Opdrachtnemer dan wel derde(n) die niet exclusief aan de Opdrachtgever beschikbaar wordt gesteld en welke door Opdrachtnemer (specifiek) ten behoeve van het gebruik door Opdrachtgever zullen worden aangepast. Het intellectueel eigendom ligt bij de Opdrachtnemer dan wel derde(n).

Artikel 2 Intellectuele eigendomsrechten

1. Alle intellectuele eigendomsrechten die ten aanzien van het Product waar en wanneer ook kunnen worden uitgeoefend, berusten bij:

   a. De Opdrachtgever voor zover het betreft (onderdelen van) het Product die specifiek voor de Opdrachtgever zijn of worden ontworpen of vervaardigd en/of onder leiding of toezicht van de Opdrachtgever dan wel aan de hand van diens instructies of ontwerpen zijn gerealiseerd. Voor zover nodig worden deze rechten op grond van de Overeenkomst door de Opdrachtnemer aan de Opdrachtgever overgedragen welke overdracht reeds nu voor alsdan door de Opdrachtgever wordt aanvaard;

   b. De Opdrachtnemer of een derde in alle overige gevallen. Opdrachtnemer verleent in dat geval aan de Opdrachtgever een nader bij de Overeenkomst te bepalen niet exclusief recht tot gebruik van (onderdelen van) het Product dat in ieder geval toereikend is voor nakoming van het in de Overeenkomst(en) bepaalde.

2. Door ondertekening van de Overeenkomst worden de in lid 1 sub a bedoelde rechten aan de Opdrachtgever overgedragen. Voor zover voor de overdracht van die rechten op enig moment een nadere akte is vereist, stellen de Opdrachtgever en de Opdrachtnemer deze akte op.

Opdrachtnemer machtigt voor zover nodig Opdrachtgever hierbij tevens onherroepelijk om de overdracht van deze intellectuele eigendomsrechten in de desbetreffende registers in of over te (doen) schrijven.

3. Bij verschil van mening tussen partijen over intellectuele eigendomsrechten op (onderdelen van) het Product wordt er, behoudens tegenbewijs, vanuit gegaan dat die rechten bij de Opdrachtgever berusten. De Opdrachtgever mag ongeacht de uitkomst van dat geschil voortgaan met het overeengekomen gebruik.

4. De Opdrachtnemer heeft een inspanningsverplichting, voor zover nodig, om mede namens de door hem ingezette (zelfstandige) hulppersonen, afstand te doen van alle eventueel aan hem toekomende zogenoemde persoonlijkheidsrechten als bedoeld in artikel 25 lid 1, sub a t/m c Auteurswet, in de mate waarin die regelgeving zodanige afstand toelaat. De Opdrachtnemer garandeert de Opdrachtgever bevoegd te zijn om mede namens zijn (zelfstandige) hulppersonen afstand te doen.

5. De Opdrachtnemer vrijwaart de Opdrachtgever tegen aanspraken van derden terzake van een (gestelde) inbreuk op intellectuele eigendomsrechten van die derden, zulks met inbegrip van persoonlijkheidsrechten als bedoeld in artikel 25 lid 1, sub a t/m c Auteurswet, vergelijkbare aanspraken met betrekking tot kennis, ongeoorloofde mededinging en dergelijke daaronder begrepen. De Opdrachtnemer neemt op eerste verzoek van de Opdrachtgever de verdediging op zich in iedere procedure die in verband met (onderdelen van) de Programmatuur tegen de Opdrachtgever mocht worden ingesteld wegens inbreuk op de intellectuele eigendomsrechten van een derde. De Opdrachtgever zal de Opdrachtnemer in verband daarmee onverwijld van een dergelijke actie in kennis stellen en aan de Opdrachtnemer de noodzakelijke volmachten en hulp verstrekken. De Opdrachtnemer vrijwaart de Opdrachtgever tevens tegen alle schade en kosten waartoe die in een dergelijke procedure mocht worden veroordeeld alsook tegen de kosten van die procedure zelf waaronder, maar niet beperkt tot, de kosten die verband houden met het inwinnen van juridisch advies in verband daarmee.

6. De Opdrachtnemer zal in geval van een gestelde inbreuk op het intellectuele eigendomsrecht van een derde, op zijn kosten alle maatregelen treffen die kunnen bijdragen tot voorkoming van stagnatie van de bedrijfsvoering van de Opdrachtgever en tot beperking van de door de Opdrachtgever als gevolg daarvan te maken kosten en/of te lijden schade.

7. Onverminderd het bepaalde in lid 5 en lid 6 kan Opdrachtgever, indien derden hem terzake van schending van intellectuele eigendomsrechten in rechte betrekken, de Overeenkomst buiten rechte geheel of gedeeltelijk ontbinden.

Artikel 3 Gebruiksrecht

1. De Opdrachtnemer verleent aan de Opdrachtgever een Gebruiksrecht op de Standaardprogrammatuur voor een periode van 25 jaar na oplevering van het Werk. Het Gebruiksrecht omvat geen overdracht door de Opdrachtnemer aan de Opdrachtgever van octrooi-, auteurs- of merkenrechten op de betreffende Standaardprogrammatuur.

2. In het Gebruiksrecht is, zonder dat Opdrachtgever daarvoor enige additionele vergoeding verschuldigd is, in ieder geval begrepen:

    a. Het recht om alle voor de Opdrachtgever toegankelijke functionaliteiten van de Standaardprogrammatuur te gebruiken ook als die niet in de Documentatie staan vermeld;

    b. Het recht om kopieën van de Standaardprogrammatuur te vervaardigen, op te slaan, regelmatig te testen en ‘hot standby’ te houden, voor het geval van een calamiteit;

    c. Het recht om de Standaardprogrammatuur voor testdoeleinden te gebruiken;

d. Het recht om de Standaardprogrammatuur zonder enige beperking of begrenzing met betrekking tot plek, apparatuur of anderszins te gebruiken.

3. De Opdrachtgever mag kopieën van de Standaardprogrammatuur vervaardigen en in gebruik nemen zo vaak hij dat voor zijn bedrijfsvoering nodig oordeelt. Als hij daartoe overgaat en om die reden een additionele vergoeding aan de Opdrachtnemer verschuldigd is, deelt hij dat de Opdrachtnemer met bekwame spoed mee.

4. De Opdrachtgever verwijdert geen aanduidingen van eigendoms- en/of auteursrechten bij het verveelvoudigen van Standaardprogrammatuur.

5. Tot het moment van oplevering van het Werk verkrijgt de Opdrachtgever van de Opdrachtnemer een niet-exclusief recht tot het gebruik van de Standaardprogrammatuur voor installatie- en testdoeleinden. Het risico van dit Gebruiksrecht ligt bij de Opdrachtgever.

6. Indien de Opdrachtnemer gebreken in de Standaardprogrammatuur alleen herstelt door middel van het uitbrengen van Patches, heeft de Opdrachtgever gedurende de garantietermijn van artikel 5, ook al is hij met de Opdrachtnemer geen onderhoud overeengekomen, recht op de kosteloze ontvangst daarvan.

Artikel 4 Omzetting in andere gebruiksrechten

1. Indien de Opdrachtnemer het aan de Opdrachtgever verleende Gebruiksrecht op enig moment wil omzetten in een ander gebruiksrecht ten aanzien van de Standaardprogrammatuur treedt hij daarover, alsmede over de daarbij te hanteren omwisselverhouding, vooraf in overleg met de Opdrachtgever. Aan een dergelijke omzetting zijn voor de Opdrachtgever geen nadelige gevolgen van welke aard ook, verbonden.

2. Indien partijen bij het overleg bedoeld in lid 1 geen overeenstemming bereiken, mag de Opdrachtgever zijn Gebruiksrecht onverkort blijven uitoefenen.

Artikel 5 Garanties

1. De Opdrachtnemer garandeert dat hij voor zijn rekening voor de duur van 12 maanden na de datum van oplevering van het Werk, gebreken in het Product van Maatwerkprogrammatuur herstelt. Indien de Opdrachtgever een beroep wil doen op deze garantie, stelt hij de Opdrachtnemer daarvan schriftelijk en in spoedgevallen telefonisch op de hoogte. De Opdrachtnemer herstelt gebreken onverwijld rekening houdend met de ernst en de aard daarvan. Herstel vindt plaats in overleg met de Opdrachtgever. Na herstel dient Opdrachtnemer het aangepaste Product van Maatwerkprogrammatuur op te leveren aan Opdrachtgever. Het aangepaste Product van Standaardprogrammatuur waarin aanpassingen specifiek ten behoeve van Opdrachtgever zijn gedaan dient conform artikel 7 in depot te worden afgegeven.

2. De in lid 1 bedoelde garantie geldt niet voor zover de Opdrachtnemer aantoont dat een gebrek is ontstaan als gevolg van een, zonder zijn toestemming, door Opdrachtgever of een door deze ingeschakelde derde in door hem geleverde delen van de Programmatuur aangebrachte wijziging. De garantie geldt evenmin indien een gebrek aantoonbaar het gevolg is van onjuist, onzorgvuldig of ondeskundig gebruik van door hem geleverde onderdelen van Programmatuur door de Opdrachtgever.

Artikel 5a Eisen aan het Product

1. De Maatwerkprogrammatuur bevat geen technische voorzieningen, functies of andere vreemde elementen die op enig moment, al dan niet tijdelijk, aan het overeengekomen gebruik in de weg (kunnen) staan.

2. Indien Opdrachtnemer niet de rechthebbende van de Standaardprogrammatuur is, is hij door rechthebbende gemachtigd om namens deze Gebruiksrechten aan derden te verschaffen. De Opdrachtnemer verstrekt de Opdrachtgever op verzoek een kopie van die machtiging.

3. Opdrachtnemer zal desgevraagd onderhoud plegen op de door hem geleverde Maatwerkprogrammatuur door middel van een nog overeen te komen onderhoudscontract.

Artikel 6 Verstrekken Installatiekopie

1. De Opdrachtnemer verstrekt de Opdrachtgever een Installatiekopie van de geïnstalleerde versie van de Standaardprogrammatuur waarin aanpassingen zijn gedaan specifiek ten behoeve van de Opdrachtgever bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk. De Opdrachtnemer dient van de Installatiekopie van de Standaardprogrammatuur een hash waarde te genereren met gebruik van hash algoritme SHA-256.

Artikel 7 Escrow

1. COTS Programmatuur valt buiten de scope van Escrow.

2. De Opdrachtnemer voorziet voor de duur van 25 jaar na oplevering van het werk in Escrow voor Standaardprogrammatuur waarvan het intellectueel eigendom bij de Opdrachtnemer ligt en waarin aanpassingen specifiek ten behoeve van de Opdrachtgever zijn gedaan.

3. Van Standaardprogrammatuur waarin aanpassingen zijn gedaan specifiek ten behoeve van de Opdrachtgever dient het Product gedeponeerd te worden bij de Escrow agent doch uiterlijk bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk. Dit wordt bepaald door de Opdrachtgever.

4. De Opdrachtgever is gerechtigd de in te zetten Escrow agent te kiezen.

5. De in te zetten Escrow agent heeft expertise om het gedeponeerde Product te controleren op aanwezigheid, volledigheid en bruikbaarheid. Het Product dient hiertoe binnen de onafhankelijke omgeving van de Escrow agent gecompileerd en getest te worden. Ontbrekende of niet werkende onderdelen van het Product worden door de Opdrachtnemer gecorrigeerd en alsnog aangeleverd.

6. Escrow omvat alle niet openbaargemaakte informatie die de Opdrachtgever redelijkerwijs nodig heeft voor foutherstel, onderhoud, verder ontwikkelen en beheer van de Standaardprogrammatuur zodat hij daarvan het overeengekomen gebruik kan blijven maken. Escrow voldoet aan hetgeen dienaangaande ten tijde van het afsluiten daarvan op de Nederlandse markt gebruikelijk is.

7. De Escrow agent en de Escrow overeenkomst voorzien ten minste in het volgende:

   - Deponering van Materialen
   - Deponering van de Installatiekopie bij oplevering van het Werk of ingebruikneming van onderdelen van het Werk
   - Deponering van de hash waarde
   - Verificatie van de gedeponeerde Materialen
   - Verplichtingen van Escrow agent
   - Geheimhouding
   - Dat op de Intellectuele Eigendomsrechten geen pandrecht of beslag rust
   - Afgifte van het gedeponeerde
   - Garanties
   - Aansprakelijkheid

- Duur

8. De Opdrachtnemer levert Opdrachtgever nu voor alsdan, onder voorwaarde dat het gedeponeerde Product door de Escrow agent wordt vrijgegeven aan de Opdrachtgever conform de nog te sluiten Escrow overeenkomst, een gebruiksrecht op het Product om het eigenhandig en naar eigen inzicht te (laten) gebruiken, onderhouden, door ontwikkelen en beheren.

Artikel 8 Verbeterde en Nieuwe versies Standaardprogrammatuur

1. De Opdrachtnemer zorgt voor een consistent versiebeleid gedurende de periode van 25 jaar na oplevering van het Werk. Daarbij geldt als uitgangspunt dat Verbeterde en Nieuwe versies tijdig beschikbaar komen bij gebreken.

2. Tussentijdse wijzigingen in Programmatuur maken zoveel mogelijk onderdeel uit van Verbeterde en Nieuwe versies.

3. De Opdrachtnemer stelt de Opdrachtgever op verzoek kosteloos een exemplaar van een Nieuwe versie ter beschikking voor test- en evaluatiedoeleinden.

4. Indien is overeengekomen dat de Opdrachtnemer de Programmatuur installeert, geldt deze verplichting tevens voor Nieuwe versies die de Opdrachtgever in gebruik wil nemen.

5. Indien de Opdrachtnemer er voor kiest om in plaats van een Nieuwe versie andere Programmatuur uit te brengen en te stoppen met Verbeterde en Nieuwe versies van de bij de Opdrachtgever in gebruik zijnde Programmatuur, kan de Opdrachtgever aanspraak maken op een Gebruiksrecht op die nieuwe Programmatuur tegen de in de Overeenkomst vastgelegde voorwaarden voor een Nieuwe versie.

Artikel 9 Levering Maatwerkprogrammatuur

1. De Opdrachtnemer dient bij oplevering of ingebruikneming van onderdelen van het Werk van Maatwerkprogrammatuur het Product te leveren.

2. De Opdrachtnemer dient bij oplevering of ingebruikneming van onderdelen van het Werk een kopie te verstrekken van de geïnstalleerde versie van het Product van de Maatwerkprogrammatuur. Van de geïnstalleerde versie van het Product van de Maatwerkprogrammatuur dient een hash waarde te worden gegenereerd met gebruik van hash algoritme SHA-256 en meegeleverd te worden aan Opdrachtgever.

3. De Opdrachtgever heeft het recht om het geleverde Product van Maatwerkprogrammatuur zelf of door een derde partij te (laten) beoordelen op aanwezigheid, volledigheid en bruikbaarheid.

Bijlage CSR 20 Camera’s en omgang met camerabeelden van de verkeersregistratiesystemen

CSR 20.1 Doelstelling

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.

Deze 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 AVG beveiligd worden.

Medewerkers van de Opdrachtnemer (die beheer- en onderhoudswerkzaamheden verrichten aan camera’s en systemen die camerabeelden opslaan, verwerken of distribueren) dienen bewust te zijn 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. De verwerking van beelden en alle handelingen van medewerkers daaromtrent, dienen in lijn met de AVG plaats te vinden.

CSR 20.2 Best practice

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

a. Alleen geautoriseerde medewerkers van de Opdrachtnemer mogen beheer- en onderhoudswerkzaamheden uitvoeren aan camera’s en systemen die camerabeelden opslaan;
b. 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;
c. Zonder uitdrukkelijke toestemming van de Opdrachtgever worden camerabeelden niet vernietigd, verwijderd of verstrekt aan derden of gebruikt voor persoonlijke of bedrijfsdoeleinden;
d. 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;
e. 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;
f. Indien onregelmatigheden worden geconstateerd rondom de inzet, werking en opslag van camerabeelden dient dit direct als beveiligingsincident bij de Opdrachtgever gemeld te worden.

Bijlage CSR 21 Uniform aanleveren van incidentrapportages

Cybersecurityincidenten dienen te worden gerapporteerd. Daarnaast dient maandelijks een overzicht te worden gestuurd van alle incidenten. De rapportagestructuur is te vinden in de hiernavolgende paragrafen.

CSR 21.1 Formulier voor rapportage van een cybersecurityincident

Dit formulier dient zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar: EMAILADRES@rws.nl

ALGEMENE INFORMATIE	
Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Naam rapporteur:	
Functie rapporteur:	
Organisatie rapporteur:	
Telefoonnummer:	

Rapporteert hiermee het volgende cybersecurityincident:

ALGEMENE INFORMATIE INCIDENT	
Soort incident[6]:	
Incident is opgemerkt op:	[jjjjmmdd/uu:mm]
Incident opgemerkt door:	[indien ander dan rapporteur]
Is het object nog operationeel:	Ja/Nee
Opschaling incident response team nodig:	Ja/Nee

DETAIL INFORMATIE INCIDENT	
Beschrijving van het incident[7]:	
Analyse van het incident:	
Is de dreiging ingesloten:	Ja/Nee
Hoe is de dreiging ingesloten:	
Is de dreiging bestreden:	Ja/Nee
Hoe is de dreiging bestreden:	
Is herstel nodig:	Ja/Nee
Welk herstel is nodig:	

[6] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[7] Een korte, duidelijke beschrijving van het incident, verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en RWS) betreffende het incident.

CSR 21.2 Formulier voor periodieke rapportage van cybersecurityincidenten

Dit formulier dient aan het begin van elke maand zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar: EMAILADRES@rws.nl

Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Rapporteur:	[naam, functie en bedrijf van degene die het rapport opmaakt]
Periode:	[maand waarop deze rapportage betrekking heeft]

De volgende cybersecurityincidenten (inclusief hun afhandeling) hebben plaatsgevonden in de hiervoor genoemde periode:

No	**Datum/tijd incident: [jjjjmmdd/uu:mm]**	**Soort incident[8]:**	**Afgehandeld (J/N):**	**Datum/tijd afgehandeld:**	**Uitleg/opmerkingen m.b.t. incident en afhandeling[9]:**
1					
2					
3					
4					
5					

[8] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[9] Een korte, duidelijke beschrijving van het incident, incident afhandelingsnummer/verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en RWS) betreffende het incident, en hoe het incident is opgelost.

Bijlage CSR 22 Virtualisatie

CSR 22.1 Doelstelling

Virtualisatie wordt steeds vaker toegepast binnen de IA-omgeving. Vaak gebeurt dit om de beschikbaarheid van verouderde toepassingen of systemen te verhogen. Het is van belang dat virtualisatie op een cyberveilige wijze wordt ingezet en dat toepassing ervan geen nieuwe kwetsbaarheden en dreigingen introduceert.

CSR 22.2 Best Practice

Indien virtualisatie wordt toegepast gelden de volgende minimale best practices:

a. Voorafgaand aan de inzet van virtualisatie wordt een risicoanalyse uitgevoerd om de risico's van zowel virtualisatie, als het niet virtualiseren in kaart te brengen;
b. Bij toepassing van virtualisatie dient de zonescheiding in stand te blijven;
c. Security functies draaien op fysiek gescheiden virtualisatieplatformen;
d. Safety functies draaien op fysiek gescheiden virtualisatieplatformen;
e. Systeem hardening wordt toegepast op de virtualisatieomgeving, waarbij:
    i. Alleen de noodzakelijke Operating System (OS) componenten en services zijn geactiveerd;
    ii. Verbindingen met onnodige fysieke apparaten vanuit Virtual Machines (VM's) zijn verboden;
    iii. Filesharing tussen host en gast OS is gedeactiveerd;
    iv. Het gebruik van resources door individuele VM's is gelimiteerd;
    v. Zowel gast als host OS's net als de fysieke systemen regelmatig worden gepatcht;
    vi. Gewerkt wordt met minimale privileges;
f. Administrators kunnen uitsluitend gebruik maken van een persoonlijk account voor beheertaken;
g. Zowel het host OS als de gast OS's worden centraal gelogd;
h. Productie en testomgevingen voor VM's zijn gescheiden;
i. Bij toepassing van virtualisatie voor de IA dienen algemene best practices m.b.t. virtualisatie voor IV te worden gevolgd, voor zover deze de belangen van IA niet schaden.

Bijlage CSR 23 Verwijdering en vernietiging van informatie en apparatuur

CSR 23.1 Doelstelling

Indien apparatuur uit de IA omgeving met opslagmedia wordt verwijderd of hergebruikt, moet er op toegezien worden dat er geen gevoelige gegevens of in licentie gegeven software op de opslagmedia achterblijft. Denk hierbij bijvoorbeeld aan gegevensdragers zoals harde schijven, maar ook aan PLC's of IoT apparatuur. Het is van belang dat alle informatie die aanwezig is op apparatuur op zorgvuldige wijze wordt verwijderd wanneer een apparaat uit de IA omgeving wordt gehaald en afgevoerd of hergebruikt. Daarnaast dient vertrouwelijke informatie in de IA omgeving die niet meer nodig is vernietigd te worden.

CSR 23.2 Best Practice

Bij de best practices wordt er onderscheid gemaakt tussen apparatuur die wordt hergebruikt en apparatuur die wordt vernietigd enerzijds en fysieke documenten anderzijds. De volgende minimale best practices zijn van toepassing:

CSR 23.2.1 Verwijdering gegevens bij hergebruik apparatuur

Indien apparatuur wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. Vertrouwelijke informatie wordt tenminste 3 maal volledig overschreven met verschillende bitpatronen, waaronder 2 vaste patronen en één random patroon;
b. Niet vertrouwelijke informatie wordt tenminste 1 maal volledig overschreven met een random bitpatroon;
c. Er wordt gecontroleerd of de gegevens onherstelbaar zijn verwijderd;
d. Indien volledig overschrijven van de informatie niet mogelijk is, dient de gegevensdrager te worden vernietigd.

CSR 23.2.2 Verwijdering gegevens bij vernietiging apparatuur

Indien apparatuur niet wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. De informatie wordt middels een degausser verwijderd door een hiertoe gecertificeerd bedrijf, of;
b. Het apparaat wordt versnipperd door een hiertoe gecertificeerd bedrijf.

CSR 23.2.3 Verwijdering van fysieke informatie (documenten)

Verwijdering van fysieke documenten met daarop vertrouwelijke informatie vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Bij versnippering wordt er gebruik gemaakt van apparatuur waarbij de mate van versnippering (snippergrootte) in overeenstemming is met het vertrouwelijkheidsniveau van de informatie.

Bijlage A Begrippenlijst

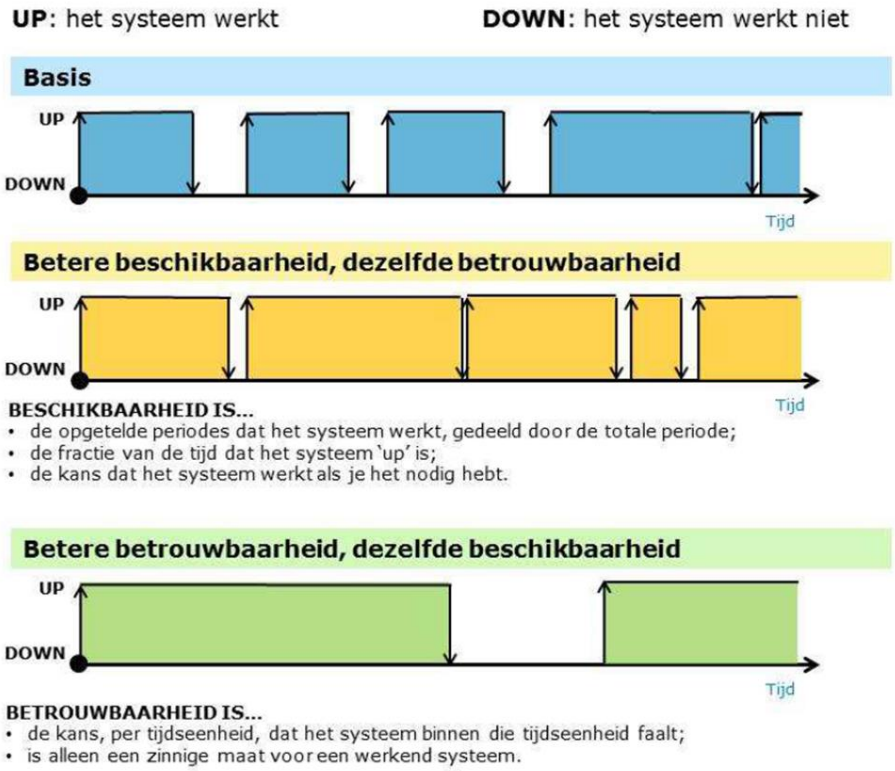
Bedrijfsmiddel
Apparatuur met informatie verwerkende en of opslag capaciteit, software die waarde vertegenwoordigt voor de organisatie en producten waarmee fysieke en of logische toegang tot ruimten en informatiesystemen verkregen kan worden.

Beheerobject
Afgebakende eenheid die bestaat uit een samenhangend geheel van elementen met één of meer autonome functies, bijvoorbeeld een tunnel, sluis, brug, kering, verkeerscentrale etc.

Beschikbaarheid (IA)
De fractie van de tijd dat een systeem werkt, of "up" is. Ofwel de opgetelde periodes (tijd) dat een systeem werkt, gedeeld door de totale periode (tijd).

Betrouwbaarheid (IA)
De kans, per tijdseenheid, dat een systeem binnen die tijdseenheid faalt.

Afbeelding: visualisatie onderscheid beschikbaarheid en betrouwbaarheid



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

Cybersecurity weerstandsniveau
Het vermogen om weerstand te bieden tegen aanvallen die bedoeld zijn om zich met geweld of manipulatie toegang fysiek dan wel digitaal te verschaffen tot ruimten en tot de informatievoorziening.

Explain
Een plausibel gemotiveerde tijdelijke afwijking ten aanzien van de eisen en maatregelen uit de BIO of de Cybersecurity Implementatierichtlijn Objecten waarvan het risico als gevolg van de afwijking geaccepteerd is.

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). PA en OT zijn synoniemen voor IA.

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.

IoT
Het Internet-of-Things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.

Kwetsbaarheid
Een kwetsbaarheid is een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.

Risico
De kans dat de dreiging optreedt en het verlies (of impact) realiteit wordt.

Risicoanalyse
Een methode die informatie oplevert, waarmee het management in staat wordt gesteld te beslissen welke risico’s, of weke combinaties van risico’s, een te grote potentiële schade vormen en met welke maatregelen deze risico’s teruggedrongen kunnen worden.

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

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

Vitale processen
Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur.

Bijlage B Cybersecurity Dossier / Cybersecurity Beveiligingsplan

De template voor het Cybersecurity Dossier / Cybersecurity Beveiligingsplan wordt op verzoek door het door het Security Centre van CIV beschikbaar gesteld.

Bijlage C Best practice voor risico inschatting bij CSIR afwijkingen

Het is van belang dat een juiste risico inschatting en afweging kan worden gemaakt indien er afwijkingen zijn aan de CSIR. Deze bijlage biedt hiervoor een best practice.

RWS hanteert de formule risico = kans x impact voor het bepalen van eventuele risico's.
De kans is de waarschijnlijk dat de dreiging zich zal manifesteren en dat de kwetsbaarheid wordt benut door het ontbreken van Baseline Beveiliging IA controls of maatregelen uit de CSIR.

Voor de bepaling van het risico dienen de volgende stappen gevolgd te worden. In de **eerste stap** wordt de kanswaarde aan de hand van onderstaande tabel bepaald.

De kans score kan bepaald worden aan de hand van de dreiging en bijbehorende kwetsbaarheid of er kan simpelweg aansluiting gezocht worden bij de kans scores zoals opgenomen en toegepast binnen de specifieke dreigingsanalyse voor RWS.

Stap 1: De kans score
De kans score of waarde wordt uitgedrukt in een vijfpuntschaal.

De kans of waarschijnlijkheid dat de dreiging zich zal manifesteren in de komende periode		Omschrijving kans en daarmee het benutten van de kwetsbaarheid
1	Verwaarloosbaar *t > 5 jaar*	De kans en daarmee het falen van de functie van het object wordt niet binnen 5 jaar verwacht;
2	Klein (*3 jaar < t ≤ 5 jaar*)	De kans en daarmee het falen van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht;
3	Middelmatig (*2 jaar < t ≤ 3 jaar)*	De kans en daarmee het falen van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht;
4	Groot (1 jaar < *t ≤ 2 jaar*)	De kans en daarmee het falen van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht;
5	Zeker (*t ≤ 1 jaar)*	De kans en daarmee het falen van de functie van het object wordt tussen nu en 1 jaar verwacht;

De manifestatie van de dreiging en benutting van de kwetsbaarheid zal leiden tot een impact voor RWS die uitgedrukt kan worden in een gevolgschade en is daarmee **de tweede stap** in het bepalen van het cybersecurity risico.

Stap 2: Gevolgschade/Impact
Bij het manifest worden van de dreiging en kwetsbaarheid zullen als gevolg van het niet of afwijkend invullen van de Baseline beveiliging IA controls en of CSIR maatregelen security (Se) maatregelen ongewenste uitwerkingen op de RAMSSHEEP aspecten van IA systemen verwacht kunnen. Ontbrekende maatregelen zullen in eerste instantie leiden tot ongewenste negatieve uitwerkingen op de betrouwbaarheid (R), availability (A), maintainability (M) en safety (veiligheid). De negatieve uitwerking op de aspecten R, A, M en S van IA systemen zullen vervolgens ook tot negatieve effecten op de overige aspecten leiden. De gevolgschade wordt conform de RWS handleiding Prestatiegestuurde Risicoanalyse (PRA) uitgedrukt in een viertal gevolgklassen.

Betrouwbaarheid' (R):
Availability (Beschikbaarheid) (A):
Maintainability (Onderhoudbaarheid) (M):
Safety (veiligheid) (S):
Security (Beveiliging) (Se);
Health (Gezondheid) (H):
Environment (Omgeving en Milieu) (E):
Economics (Levensduurkosten) (€):
Politics (Politiek) (P):

	Gevolgklasse			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
R	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de betrouwbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
A	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een verwaarloosbare invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object maar heeft een minimale invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de beschikbaarheid van het betreffend object en heeft catastrofale negatieve invloed op de hoofdfunctie.
M	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium verwaarloosbaar moelijker uitgevoerd kan worden binnen de randvoorwaarden van gebruik.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium minimaal moeilijker uitgevoerd kan worden binnen de randvoorwaarden van het gebruik.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen ernstige negatieve invloed heeft op de prestaties van de netwerkschakel.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en maakt dat onderhoud in een later stadium niet uitgevoerd kan worden binnen de randvoorwaarden van gebruik, hetgeen catastrofale negatieve invloed heeft op de prestaties van de netwerkschakel.
S	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft een verwaarloosbare invloed op gebruiksveiligheid van het object, maar dit blijft	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en leidt tot een situatie die de geaccepteerde grenzen voor gebruiksveiligheid benaderd en leidt daardoor	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en leidt tot het niet voldoen aan gestelde eisen ten aanzien van gebruiksveiligheid wat daardoor leidt tot een	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft een catastrofaal negatief effect op de gebruiksveiligheid wat leidt tot extra dodelijk gevaar bij normaal gebruik.

	Gevolgklasse			
	Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
	binnen geaccepteerde grenzen.	tot een minimaal aantal extra ongelukken met tijdelijke gezondheidsschade of letsel zonder verzuim.	ernstige toename van het aantal ongelukken met blijvend letsel of met blijvende gezondheidsschade.	
Se	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object maar heeft een minimale invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object en heeft een minimale negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffend object die tot security incidenten leiden en heeft hiernaast ernstige negatieve invloed op de hoofdfunctie.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft negatieve invloed op de fysieke en of logische toegangsbeveiliging van het betreffende object die tot security incidenten leiden en heeft hiernaast catastrofale negatieve invloed op de hoofdfunctie en of de prestaties van de netwerkschakel.
H	Het niet uitvoeren van de onderhoudsmaatregel heeft een verwaarloosbare negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een minimale negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een ernstige negatieve invloed op de gezondheid.	Het niet uitvoeren van de onderhoudsmaatregel heeft een catastrofale negatieve invloed op de gezondheid en veroorzaakt overlijden.
E	Het niet uitvoeren van de maatregelen heeft een verwaarloosbaar negatief effect op het gebruik.	Het niet uitvoeren van de maatregel heeft een beperkt negatief effect op het gebruik en beperkt zich tot consequenties voor het lokale netwerk.	Het niet uitvoeren van de maatregel heeft een ernstig negatief effect op het gebruik en heeft consequenties voor het regionale netwerk.	Het niet uitvoeren van de maatregel heeft een catastrofaal negatief effect op het gebruik en heeft consequenties voor het landelijke netwerk.
€	Uitstel geeft < 50 k Euro aan extra onderhoud/claims/inspect ies.	Uitstel geeft < 500 k Euro aan extra onderhoud/claims/inspecti es.	Uitstel geeft < 1000 k Euro aan extra onderhoud/claims/inspecti es.	Uitstel geeft > 1000 k Euro aan extra onderhoud/claims/inspecti es.
P	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en heeft verder geen politieke consequenties.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor verscherpte controles door toezichthouders.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor negatieve media berichtgeving die tot kamer vragen kunnen leiden.	Het niet (binnen het geplande jaar) uitvoeren van de (onderhouds) maatregel voor cybersecurity leidt tot een niet compliancy registratie en rapportage en de positie van DG, de Minister of Staatssecretaris staat ter discussie.

In de derde stap wordt de risicoscore afgebeeld in de risicomatrix of heat map waarbij op de ene as de impact/gevolgschade wordt uitgedrukt en op de andere as de kans (waarschijnlijkheid) dat de dreiging en kwetsbaarheid manifest wordt.

Stap 3: Risicomatrix en risicoscore
De risicomatrix is hieronder weergegeven. De risicoscore wordt eenvoudig bepaald door kans- en gevolgscore met elkaar te vermenigvuldigen. De hoogte van dit getal geeft aan hoe noodzakelijk een beheersmaatregel is. Hierin worden drie niveaus onderscheiden: het rode, oranje of groene gebied.

1. Onacceptabel — Risicoscore 15 t/m 20
Er moeten direct beheersmaatregelen worden getroffen om het risico te beheersen.

2. Ongewenst — Risicoscore 5 t/m 12
Er moet ofwel een beheersmaatregel worden getroffen om het risico te beheersen ofwel worden aangetoond waarom dit niet haalbaar/noodzakelijk is

3. Acceptabel — Risicoscore 1 t/m 4
Er hoeft geen maatregel te worden getroffen om het risico te beheersen. Bij falen van de functie van het object worden de gebruikelijke acties ondernomen voor (functie-)herstel.

		Impact			
		Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
Kans	Verwaarloosbaar (1)	Acceptabel (1)	Acceptabel (2)	Acceptabel (3)	Acceptabel (4)
	Klein (2)	Acceptabel (2)	Acceptabel (4)	Ongewenst (6)	Ongewenst (8)
	Gemiddeld (3)	Acceptabel (3)	Ongewenst (6)	Ongewenst (9)	Ongewenst (12)
	Groot (4)	Acceptabel (4)	Ongewenst (8)	Ongewenst (12)	Onacceptabel (16)
	Zeker (5)	Ongewenst (5)	Ongewenst (10)	Onacceptabel (15)	Onacceptabel (20)