Cybersecurity Implementatierichtlijn Objecten – RWS

Uitgegeven door	PRIA / CIV-IRN Security Center
Steller	Turabi Yildirim
Datum	02 december 2013
Status	Definitief
Vertrouwelijkheid	RWS Ongeclassificeerd
Informatieklasse	RWS-O
Versie	1.01

Vaststelling
11-12-2013

Beoordeeld door:

Hellen Havinga
Senior Adviseur PRIA

Goedgekeurd door:

Olaf van Duin
Programmadirecteur PRIA

Vastgesteld door:

Rein van der Kluit
HID RWS Centrale Informatie Voorziening

Inhoudsopgave

1 Inleiding

Cybersecurity is er op gericht om uitval, verstoring en misbruik van ICT-systemen te voorkomen en daarmee bij te dragen aan de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatievoorziening (IV) en de Industriele Automatisering (IA) van RWS.

1.1 Baseline Informatiebeveiliging RWS

De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor. De BIR biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van het Rijk. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

In het beveiligingsbeleid van IenM wordt de Baseline Informatiebeveiliging Rijksdienst (BIR) gehanteerd als het te volgen Tactisch Normen Kader voor de beveiliging van de IV. De BIR is daarmee ook kaderstellend voor RWS. De BIR hoofdstukken en paragrafen worden integraal aangehouden voor de vertaalslag en invulling van de beveiliging van de IV van RWS. De Baseline Informatiebeveiliging RWS (BIR RWS) is het resultaat van de vertaalslag en invulling van de BIR voor de beveiliging van de IV van RWS.

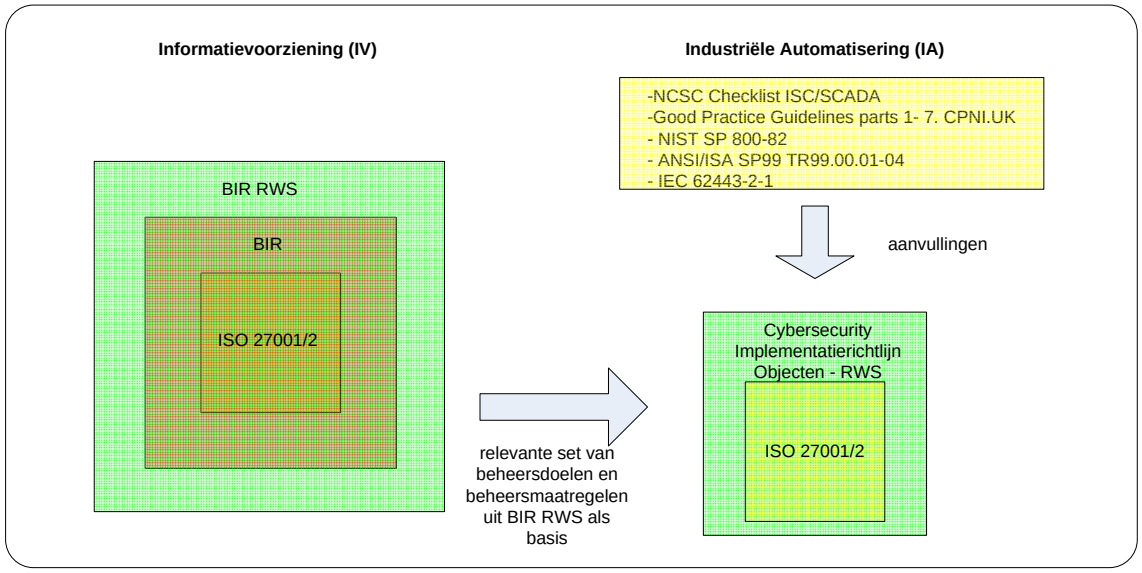
1.2 Cybersecurity Implementatierichtlijn Objecten - RWS

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

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

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

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

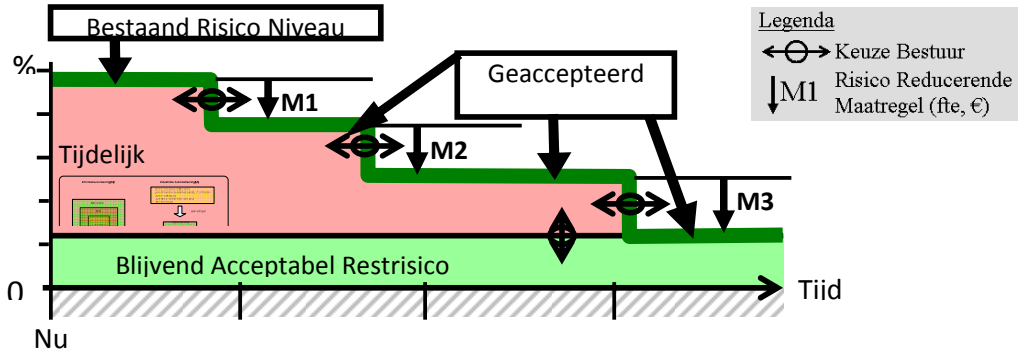


De Cybersecurity Implementatierichtlijn Objecten - RWS is een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR RWS en de NCSC Checklist beveiliging ICS/SCADA systemen voor de beveiliging van objecten RWS. Waar nodig zijn aanvullingen gedaan uit good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

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

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

Mitigatiestrategie – Sturing op top 10 maatregelpakketten



1.3 Instructie voor toepassing

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

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

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

Cybersecurity weerstandsvermogen in Ketens: Elke keten is zo sterk als de zwakste schakel. Indien de bediening of het beheer van object A wordt gedaan vanuit een initieel lager geclassificeerd object B, wordt de classificatie van dat object B verhoogd tot het cybersecurity weerstandsniveau van object A.

Als een RWS object nog niet voorzien is van een cyber-classificatie dient er contact gezocht te worden met de afdeling Security Center van RWS-CIV-IRN voor advies en correcte indeling qua cybersecurity weerstandsniveau.

In het geval dat er helemaal geen object uit de infraclassificatie lijst objecten voorkomt in de scope van de overeengekomen dienstverlening dan dient voor de beveiliging van de ICT-, ICS/SCADA-, DVM-systemen en datanetwerkcomponenten binnen de Infrastructuur RWS het Cybersecurity weerstandniveau van 1 te worden aangehouden.

Voorbeeld

Uitgaande van een specifieke tunnel met cyber-classificatie B (volgens Infraclassificatie) dienen alle generieke beheersdoelen uitgewerkt te worden in het beveiligingsplan van Opdrachtnemer. Voor de tunnel dienen de generieke beheersdoelen met als uitgangspunt cybersecurity weerstandsniveau 3 in bovenstaand tabel aangevuld te worden met specifieke maatregelen uit de maatregelpakketten die te vinden zijn in hoofdstuk 3 van dit document. Bij mogelijke overlap tussen de generieke beheersdoelen en de specifieke aanvullende maatregelen uit de maatregelpakketten dienen de specifieke maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens de bovenliggende generieke beheersdoel en of beheersmaatregel ingevuld.

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

1.4 Structuur

Hoofdstuk 2 beschrijft de relevante set van beheersdoelen en beheersmaatregelen die afgeleid zijn uit de BIR (RWS). Dit zijn de meer generieke geformuleerde beheersdoelen en beheersmaatregelen in de vaste hoofdstuk- en paragraaf indeling van de BIR (RWS). Binnen de hoofdstuk structuur van de BIR RWS zijn tevens de relevante beheersdoelen en beheersmaatregelen uit de NCSC Checklist beveiliging ICS/SCADA systemen geïntegreerd. Indien noodzakelijk wordt vanuit de generieke beheersdoel doorverwezen naar de specifieke maatregelpakketten waar een verdieping plaatsvindt in de maatregelenset en dit is weer afhankelijk van het risico en het cybersecurity weerstandsniveau dat gehaald moet worden.

Hoofdstuk 3 beschrijft de specifieke maatregelpakketten. De specifieke maatregelpakketten zijn een aanvulling en verdieping op de generieke beheersdoelen en beheersmaatregelen uit hoofdstuk 2. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS hanteert. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS. Afhankelijk van de infraclassificatie en de daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maatregelpakketten is gebruik gemaakt van de NCSC Checklist beveiliging ICS/SCADA systemen en overige good practices voor de beveiliging van IA en ICS/SCADA systemen.

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

2 Generieke beheersdoelen en beheersmaatregelen

Het Beveiligingsbeleid van IenM geeft aan dat de dienstonderdelen daar waar nodig aanvullingen dienen te plegen op de BIR om de beveiligingsrisico's in het eigen werkveld zoals de IA te mitigeren.

De BIR (RWS) is vanwege de interne gerichte formulering van beheersdoelen en beheersmaatregelen die veelal gelinkt worden aan de interne rolhouders en organisatorische inbedding niet zonder meer geschikt voor toepassing in projecten en in uitbestedingstrajecten. Een vertaalslag is nodig van de BIR (RWS) beheersdoelen en beheersmaatregelen naar een meer pragmatische en operationele toepassing.

De Cybersecurity Implementatierichtlijn Objecten - RWS is dan ook niet meer dan een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR RWS en de "NCSC Checklist beveiliging ICS/SCADA systemen" voor de beveiliging van objecten. Waar nodig zijn aanvullingen gedaan uit good practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen. De formulering van de beheersdoelen en beheersmaatregelen zijn generiek van aard en daardoor geschikt voor zowel RWS interne doelgroepen zoals objectbeheerders en projecten als voor gebruik bij inkooptrajecten, contracten, vraagspecificaties en uitvoering van werk door marktpartijen. Indien nodig wordt verwezen naar aanvullende beheersdoelen en beheersmaatregelen die in hoofdstuk 3 staan beschreven. Op basis van de risico mitigatiestrategie en de infraclassificatie objecten kunnen aanvullende specifieke maatregelen nodig zijn om invulling te geven aan de generiek geformuleerde beheersdoelen en beheersmaatregelen in dit hoofdstuk.

BIR-(RWS) indeling		**Generieke beheersdoelen en beheersmaatregelen**
B-1 A5.1.1	**Hoofdeis Cybersecuritybeleid**	Opdrachtnemer conformeert zich aan het Cybersecuritybeleid van Opdrachtgever door invulling te geven aan de Cybersecurity beheersdoelen en maatregelen zoals beschreven in de overeenkomst en de specifieke aanvullende beheersdoelen en maatregelen die zijn beschreven in de Cybersecurity Implementatierichtlijn Objecten - RWS.
	Invulling	Middels beheersmaatregelen uit Cybersecurity Implementatierichtlijn Objecten - RWS.
B-2	**Code voor Informatie-beveiliging**	Voor de invulling van de beheersdoelen dient Opdrachtnemer beheersmaatregelen te implementeren die volgen uit de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever. Indien de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever niet voorziet in specifieke beheersmaatregelen voor de invulling van de beheersdoelen van Opdrachtgever dan dient de Code voor Informatiebeveiliging - NEN-ISO/IEC 27002-2005 (of de meest recente versie hiervan) aangehouden te worden voor de te nemen beheersmaatregelen in relatie tot het beheersdoel van Opdrachtgever.
	Invulling	Middels Cybersecurity Implementatierichtlijn Objecten - RWS of de beheersmaatregelen uit NEN-ISO/IEC-27002
B-3	**Gelaagde beveiliging**	Bij de keuze van de beheersmaatregelen voor de beveiliging van de infrastructuur en systemen en met name voor de ICS/SCADA toepassingen dient het principe van gelaagde beveiliging gevolgd te worden die meerdere lagen van beveiliging bewerkstelligt binnen het ontwerp en inrichting op proces-, netwerk-, systeem- en applicatieniveau.
NCSC T/O-4	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002
B-4 A5.1.2	**Evaluatie en actualisatie van Cybersecuritybeleid**	Opdrachtgever behoudt te allen tijde het recht om wijzigingen in de beheersdoelen aan te brengen als gevolg van de periodieke evaluatie van het Cybersecuritybeleid of naar aanleiding van (dreigende) incidenten. In dergelijke gevallen dient de Opdrachtnemer direct passende beheersmaatregelen te treffen.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 5.1.2, 13.1 en 13.2
B-5	**Belegging**	De Opdrachtnemer dient voor Cybersecurity de verantwoordelijkheden binnen de eigen organisatie te beleggen.

A6.1	**verantwoordelijk-heden**	
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 6.1.1 en 6.1.3
B-6 A6.1	**Borging beheersdoelen en certificering**	Opdrachtnemer dient de Cybersecurity beheersdoelen van Opdrachtgever te borgen in zijn processen/(kwaliteits)managementsysteem en kan ervoor kiezen om zich te laten certificeren conform NEN-ISO/IEC-27001. Indien voor certificering conform de NEN-ISO/IEC-27001 wordt gekozen dienen de beheersdoelen van Opdrachtgever onderdeel uit te maken van de scope van certificering.
NCSC O-1	Invulling	
B-7 A6.2.3	**Onderaanneming**	Opdrachtnemer dient alle relevante Cybersecurity beheersdoelen en maatregelen aan alle onderaannemers middels een overeenkomst op te leggen en toe te zien op naleving.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 6.2.3
B-8	**Risicomanagement**	Opdrachtnemer dient op basis van risicoanalyses en risicoafwegingen voor de Cybersecurity beheersdoelen van Opdrachtgever beheersmaatregelen te treffen.
NCSC O-2	Invulling	Conform NEN-ISO/IEC-27005
B-9 A7.1.1	**Inventarisatie Configuration Items en opname in Configuration Management Database**	Opdrachtnemer dient over een geborgde procedure te beschikken voor de inventarisatie en registratie van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden en draagt zorg dat deze informatie beschikbaar is voor andere beheerprocessen.
NCSC T/O-10	Invulling	Middels ITIL Configuration Management
B-10 A7	**Beveiliging bedrijfsmiddelen**	Opdrachtnemer dient maatregelen te nemen om de ICT- ICS/SCADA- DVM-systemen en datanetwerken te beschermen tegen verlies, vernietiging en vervalsing.
	Invulling	
B-11	**Aanvaardbaar gebruik**	Door Opdrachtgever beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICT, ICS/SCADA en

A7.1.3	**toegangsmiddelen**	ondersteunende systemen en –netwerken dienen alleen gebruikt te worden voor het doel waarvoor ze ontworpen zijn waarbij de beveiligingsmaatregelen niet omzeild mogen worden.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 7.1.3
B-12 A7.2.1	**Classificatie en beveiliging informatie**	Opdrachtnemer dient de door Opdrachtgever aangegeven classificatie en bijbehorende beveiligingsmaatregelen aan te houden voor de beveiliging van informatie.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 7.2
B-13 A8	**Bewustwording en scholing**	Opdrachtnemer dient voor bewustwording en scholing middels de beheersmaatregelen uit de Cybersecurity Implementatierichtlijn Objecten - RWS te bewerkstelligen dat werknemers en ingehuurd personeel bewust worden gemaakt en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
NCSC O-5	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen bewustwording en training” uit de Cybersecurity Implementatierichtlijn Objecten - RWS en beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 8.2.2
B-14 A8.1.2	**Gescreend personeel**	Opdrachtnemer dient werkzaamheden door gescreend personeel te laten uitvoeren. De Opdrachtnemer dient te verzorgen dat al het onderhoudspersoneel voorafgaand aan operationele inzet een geheimhoudingsverklaring heeft ondertekend en over een VOG bezit die gerelateerd is aan de beoogde werkzaamheden. Opdrachtnemer houdt hier een actuele administratie van bij. Hangende de aanvraag van een VOG kan worden volstaan met een eigen verklaring van betreffende medewerker gedurende een periode van maximaal zes weken welke niet verlengd kan worden.
	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen beheer en onderhoud uit Cybersecurity Implementatierichtlijn Objecten - RWS
B-15 A9.1.1	**Fysieke beveiliging**	De fysieke beveiliging van het object dient conform het “Handboek Security Rijkswaterstaat” te worden vormgegeven.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit het “Handboek Security Rijkswaterstaat”.
B-16 A9.1.2	**Fysieke toegangsbeveiliging**	De fysieke toegangsbeveiliging IA - ruimten binnen het object dient conform de beheersmaatregelen uit de Cybersecurity Implementatierichtlijn Objecten - RWS hoofdstuk “ Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten” ingevuld te worden.

NCSC T/O-9	Invulling	Middels beheersmaatregelen uit hoofdstuk " Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" van de Cybersecurity Implementatierichtlijn Objecten - RWS
B-17 A9.2.1	**Plaatsing en bescherming van RWS bedrijfsmiddelen**	Opdrachtnemer dient zorg te dragen dat bedrijfsmiddelen, ICT-, ICS/SCADA-, DVM-systemen en datanetwerkcomponenten zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.2.1
B-18 A9.2.3	**Voedings- en telecommunicatie-kabels**	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, dienen tegen aftapping of beschadiging te zijn beschermd.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.2.3
B-19 A10.1.1 NCSC T/O-10	**Documentatie bediening en beheer**	ICS/SCADA, beveiliging, ICT-systemen en –netwerken dienen een gedocumenteerde beheer- en bedienprocedure, onderhoud en support level te hebben.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 10
B-20 A10.1.2	**Geborgde wijzigings-procedure**	Opdrachtnemer dient conform hoofdstuk "Maatregelen gecontroleerd wijzigen" uit de Cybersecurity Implementatierichtlijn Objecten - RWS over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Wijzigingen dienen eerst in de testomgeving beproefd te worden.
NCSC T/O-10	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen gecontroleerd wijzigen" van de Cybersecurity Implementatierichtlijn Objecten - RWS en ITIL Changemanagement proces
B-21 A10.4.1	**Hardening**	ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen dienen middels beheersmaatregelen uit hoofdstuk "Bescherming tegen malware, hardening en patching" van de Cybersecurity Implementatierichtlijn Objecten - RWS te zijn gehardend door: • niet noodzakelijke netwerkservices uit te zetten • verwijderen van bekende kwetsbaarheden • alle poorten die niet nodig zijn te deactiveren/blokkeren • alle default "access points" te verwijderen • optimaal gebruik te maken van de security opties van leveranciers

	Invulling	Middels beheersmaatregelen uit hoofdstuk “Bescherming tegen malware, hardening en patching” van de Cyberscecurity Implementatierichtlijn Objecten - RWS.
B-22 A10.4.1	**Bescherming tegen malware**	Er dient een geborgde procedure en voorzieningen conform hoofdstuk “Bescherming tegen malware, hardening en patching” van de Cybersecurity Implementatierichtlijn - RWS te bestaan voor detectie en preventie tegen malware. Tevens dient Opdrachtnemer voor controle vooraf van in te zetten beheer- en onderhoudsapparatuur over een geborgde procedure en voorzieningen te beschikken voor detectie, preventie en verwijdering van malware.
	Invulling	Middels beheersmaatregelen uit hoofdstuk “Bescherming tegen malware, hardening en patching” van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-23 A10.5.1	**Back-ups en bewaartermijnen**	De integriteit en beschikbaarheid van de ICS/SCADA systemen, programmatuur en besturingssystemen dient conform hoofdstuk “Back-ups” van de Cybersecurity Implementatierichtlijn Objecten - RWS gewaarborgd te worden door het maken van back-ups om herstel na een incident of calamiteit mogelijk te maken.
	Invulling	Middels beheersmaatregelen uit hoofdstuk “Back-ups” van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-24 A10.5.1	**Back-up en recovery procedure**	Er dient conform hoofdstuk “Maatregelen Back-ups” van de Cybersecurity Implementatierichtlijn Objecten - RWS een geborgd proces te bestaan voor het jaarlijks controleren en testen van de recovery procedure en de leesbaarheid en bruikbaarheid van de ingezette media voor back-ups.
		Middels beheersmaatregelen uit hoofdstuk “Maatregelen Back-ups” van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-25 A10.7.4	**Beveiliging documentatie**	Documentatie van ICS/SCADA, beveiliging, ICT-systemen en –netwerkelementen dient beschermd te worden tegen onbevoegde toegang.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.7.4
B-26 A10.10.1	**Activiteiten in audit-logbestanden**	De activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen dienen conform de beheersmaatregelen uit hoofdstuk “Maatregelen Logging en Monitoring” van de Cybersecurity Implementatierichtlijn Objecten - RWS te worden vastgelegd in audit-logbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf

BIR 10.10		• een tot een natuurlijk persoon herleidbare gebruikersnaam of (systeem)-ID • de gebeurtenis • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
NCSC T/O-8		Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logging en Monitoring" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-27	**Geen gevoelige gegevens in logregels**	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.
		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.10.1
B-28 A10.10.1	**Bewaartermijn audit logbestanden**	Opdrachtnemer dient van de systemen met logvoorzieningen de audit logbestanden een maand te bewaren.
NCSC T/O-8		
B-29 A10.10.3	**Beveiliging logbestanden**	De Opdrachtnemer dient zorg te dragen voor de beveiliging van logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en -netwerkelementen.
NCSC T/O-8		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.10.3
B-30 A10.10.3	**Levering logfiles**	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en- netwerkelementen dienen op verzoek aan Opdrachtgever in CSV-formaat opgeleverd te worden.
NCSC T/O-8		
B-31 A11.1.1	**Toegang geautoriseerden fysiek en logisch**	Opdrachtnemer dient conform hoofdstuk "Maatregelen Logische toegang" van de Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat de fysieke toegang tot het object en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan is voor personen die hiertoe door Opdrachtgever en/of Opdrachtnemer

		geautoriseerd zijn.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen Logische toegang” van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-32 A11.2.1	**Registratie fysieke toegang**	Opdrachtnemer dient zorg te dragen voor een procedure en registratie die de lokale fysieke toegang van alle medewerkers inclusief onderaannemers tot technische ruimten regelt en dat de registratie up-to-date blijft, hetzij geautomatiseerd hetzij op papier. *Toelichting: Opdrachtnemer is, binnen de overeengekomen beheertaken, verantwoordelijk voor het onderhouden van een registratie van alle aan medewerkers - zowel van Opdrachtnemer als onderaannemers - toegekende autorisaties en toegangsmiddelen.*
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.1.2 en 11.2
B-33 A11.3.1	**Wachtwoord richtlijn**	Opdrachtnemer dient zorg te dragen dat op ICS/SCADA en ondersteunende ICT systemen en –netwerken standaard/default accounts en/of wachtwoorden uitgeschakeld zijn en gehandeld wordt conform de beheersmaatregelen uit hoofdstuk “Wachtwoord Richtlijn” van de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever.
NCSC T/O-3	Invulling	Middels beheersmaatregelen uit hoofdstuk “Wachtwoord Richtlijn” van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-34 A11.4.1	**Koppeling apparatuur**	Opdrachtnemer dient over een geborgde procedure te beschikken voor het veilig koppelen van mobiele apparatuur van derden of removable media aan locale ICS/SCADA netwerken of het RWS netwerk.
NCSC T/O-6 en 7	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.7.1
B-35 A11.4.5	**Geen directe verbinding met kantoornetwerken**	Opdrachtnemer dient zorg te dragen dat ICS/SCADA en de ondersteunende systemen en besloten (lokale) datanetwerken geen directe verbindingen hebben met kantoornetwerken.
NCSC T/O-2	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.4.5
B-36	**Minimalisatie**	Opdrachtnemer dient conform hoofdstuk “Maatregelen Netwerkkoppelingen” van de Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat het aantal netwerkkoppelingen tussen ICS/SCADA

	netwerkkoppelingen	systemen en andere netwerken beperkt blijft tot alleen de functioneel noodzakelijke
NCSC T/O-2	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Netwerkkoppelingen" van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-37	**Verboden en geautoriseerde verbindingen**	Opdrachtnemer dient zorg te dragen dat er geen Internet, draadloze (WiFi en GPRS/UMTS etc.) of inbelvoorzieningen verbonden worden met de besloten (lokale) objectnetwerken en/of hierop aangesloten systemen. Uitgezonderd zijn de netwerkverbindingen van het object met de centrale netwerkvoorzieningen van RWS en de door RWS-CIV toegestane verbindingen.
NCSC T/O-2	Invulling	
B-38	**Remote access**	Opdrachtnemer dient conform hoofdstuk "Maatregelen Logische toegang" van Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat Remote Access voor bediening en beheer tot ICT, ICS/SCADA en (ondersteunende) systemen en objectnetwerken altijd verloopt via de centrale, beveiligde en gemonitorde voorzieningen van RWS met inzet van two-factor authenticatie. De aanvraag verloopt via Opdrachtgever en conform de "Procedure Toegang derden RWS".
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logische toegang" van Cybersecurity Implementatierichtlijn Objecten - RWS en "Procedure Toegang derden RWS".
B-39	**Actuele documentatie netwerkkoppelingen**	Opdrachtnemer dient over een geborgde procedure te beschikken die: • alle wijzigingen aan het objectnetwerk bijhoudt; • de lokale objectnetwerktopologie actueel houdt; • een zodanig detailniveau heeft dat alle netwerkkoppelingen en objectnetwerkcomponenten met alle relevante informatie beschikbaar is in een CMDB.
TF 1 en 3; NCSC T/O-2	Invulling	
B-40 A11.4.6	**Compartimentering infrastructuur**	ICS/SCADA systemen dienen gebruik te maken van een eigen gecompartimenteerde infrastructuur die van de Kantoorautomatisering is afgescheiden. De scheiding kan fysiek of logisch zijn.
NCSC T/O-1	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.4.5

B-41	**Segmentering van verkeersstromen**	Binnen de locale object dataverkeersnetwerken voor ICS/SCADA systemen dient segmentering voor de datastromen voor productie, beheer en OTA toegepast te worden.
B-42	**Gebruik beveiligde communicatie protocollen**	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
B-43	**Beveiligde netwerkkoppelingen en netwerkaansluit-voorwaarden RWS**	Opdrachtnemer dient zorg te dragen dat alle netwerkkoppelingen tot het RWS netwerk en de lokale objectnetwerken strikt en uitsluitend plaats vinden via de centrale beveiligde voorzieningen en conform de NNV-aansluitvoorwaarden van RWS.
	Invulling	Conform “NNV aansluitvoorwaarden”
B-44 A11.5.2	**IAA proces**	De toegang tot gegevens, de verwerking of de uitwisseling van gegevens met derden, ICS/SCADA en ondersteunende systemen en -netwerken dient plaats te vinden na een succesvol identificatie, authenticatie en autorisatie proces.
	Invulling	
B-45 A11.2.3 & BIR 11.2.3	**Versleutelde uitwisseling en opslag van IAA gegevens**	Identificatie, authenticatie en autorisatiegegevens worden in versleutelde vorm uitgewisseld en in versleutelde vorm opgeslagen.
	Invulling	
B-46 A11.6.1	**Verboden toegang tenzij expliciet toegestaan**	Alle toegang tot informatie, systemen, ICS/SCADA en de ondersteunende systemen en -netwerken dient geweigerd te worden tenzij het expliciet is toegestaan.

NICC	Invulling	
B-47	**Lokale logische toegang**	Opdrachtnemer dient voor de lokale logische toegang tot ICT-, ICS/SCADA-systemen en lokale tunnelnetwerken over een geborgde procedure en up-to-date registratie te beschikken van uitgegeven accounts met bijbehorende rechten.
	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen Logische toegang” van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-48	**Raamwerk beveiliging webapplicaties**	Bij inzet van webapplicaties voor bediening en beheer dient het “Raamwerk beveiliging Webapplicaties” van het National Cyber Security Centrum voor de invulling van beveiliging gevolgd te worden.
	Invulling	Middels “Raamwerk beveiliging Webapplicaties” van het National Cyber Security Centrum.
B-49 A12.1.1	**Validatie controles**	Toepassingen dienen te voorzien in validatie controles om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.2
B-50	**WIB vendor requirements**	Voor leveranciers van ICS/SCADA systemen dient Opdrachtnemer waar mogelijk de vendor requirements te hanteren van de Werkgroep voor Instrument Beoordeling (WIB).
A12.5.5	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.5.5 en WIB vendor requirements versie 2.0 oktober 2010.
B-51 A12.6.1	**Respons proces op technische kwetsbaarheden**	De Opdrachtnemer dient een proces te hebben waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken en Opdrachtnemer maakt dit aantoonbaar aan Opdrachtgever.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.6
B-52 A12.6.1	**Beveiligingsupdates en patches**	Opdrachtnemer dient zorg te dragen dat ICT systemen die gekoppeld worden aan ICS/SCADA, beveiliging- en netwerkomgeving en de ICS/SCADA systemen zelf, voorzien zijn van alle recente beveiligingsupdates en patches.
NCSC T/O-5	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.4.1

B-53	**Risicoanalyse en implementatieadvies kritieke patches**	Opdrachtnemer dient conform hoofdstuk “Maatregelen bescherming tegen malware, hardening en patching” van Cybersecurity Implementatierichtlijn Objecten - RWS over een geborgde procedure te beschikken die er voor zorgt dat voor kritieke patches binnen 48 uur na melding, gerekend vanaf eerstvolgend werkdag een risicoanalyse wordt uitgevoerd en voorzien is van een implementatieadvies. Voor niet kritieke patches is de doorlooptijd voor uitvoering van risicoanalyse en implementatieadvies maximaal twee maanden. De patches worden na instemming met het implementatieadvies door Opdrachtgever conform het advies door Opdrachtnemer geïmplementeerd.
NCSC T/O-5	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen bescherming tegen malware, hardening en patchting” van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-54 A13.1.1	**Procedure incidenten informatiebeveiliging**	Opdrachtnemer dient conform implementatierichtlijn “Maatregelen Beveiligingsincidenten en Incident Response” een geborgde procedure te hebben voor het melden en oplossen van informatiebeveiligingsincidenten.
	Invulling	Middels implementatierichtlijn “Maatregelen Beveiligingsincidenten en Incident Response”
B-55 A13.1.2	**Rapportage incidenten informatiebeveiliging**	Opdrachtnemer dient aan Opdrachtgever maandelijks een rapportage te verstrekken van alle beveiligingsincidenten, en van alle maatregelen die ter zake getroffen zijn.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 13.1
B-56 A13.2.3	**Bewijsmateriaal verzamelen en bewaren**	In voorkomende gevallen dient Opdrachtnemer zijn medewerking te verlenen bij een juridische vervolgprocedure voor het verzamelen en bewaren van bewijsmateriaal.
		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 13.2.3
B-57 A4.1.3	**Continuïteit en herstel bedrijfsprocessen en -activiteiten**	Opdrachtnemer dient maatregelen te nemen om onderbreking van dienstverlening voor Opdrachtgever tegen te gaan en continuïteitsplannen te ontwikkelen voor de kritieke dienstverleningsprocessen waarmee deze beschermd worden tegen de gevolgen van omvangrijke storingen in informatiesystemen en herstel bewerkstelligd wordt.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 hoofdstuk 14
B-58	**Testen**	Opdrachtnemer dient jaarlijks de ontwikkelde continuïteitsplannen te testen om te bewerkstelligen dat ze

A14.1.5	**continuïteitsplannen**	actueel en doeltreffend blijven.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 paragraaf 14.1.5.
B-59 A15	**Vigerende wet- en regelgeving en geheimhouding**	Opdrachtnemer dient te bewerkstelligen dat informatie en persoonsgegevens overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen, worden beveiligd en geheimhouding in acht wordt genomen.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 15
B-60 A15	**Wet bescherming persoonsgegevens**	De Opdrachtnemer dient zorg te dragen voor rechtmatige verwerking en omgang met persoonsgegevens, camerabeelden en andere tot natuurlijke personen herleidbare gegevens.
	Invulling	Conform Wet bescherming persoonsgegevens
B-61 A15	**Beveiligingswerkplan en onderhoud beheersmaatregelen**	De Opdrachtnemer draagt zorg voor een up-to-date beveiligingswerkplan die op verzoek aan Opdrachtgever beschikbaar wordt gesteld en verder dienen de getroffen beheersmaatregelen voor beveiliging beheert en onderhouden te worden conform de “Cybersecurity Implementatierichtlijn Objecten - RWS hoofdstuk Maatregelen Beheer en onderhoud” van Opdrachtgever. *Toelichting: Beveiligingseisen moeten de totale keten van ontwikkeling, aanschaf, beheer, onderhoud en vervanging, etc. afdekken en het toepassen van de eisen moet in elke fase gewaarborgd zijn.*
NCSC O-3 en 4	Invulling	Middels beheersmaatregelen uit hoofdstuk “Maatregelen Beheer en Onderhoud” van Cybersecurity Implementatierichtlijn Objecten – RWS en middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 15
B-62 A15	**Audit rapportage over getroffen maatregelen**	Opdrachtnemer dient jaarlijks een audit uit te voeren op de opzet, bestaan en werking van de getroffen Cybersecurity beheersmaatregelen en rapporteert hierover aan Opdrachtgever.
NCSC-O-5	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 paragraaf 15.3
B-63	**Wbp bewerkers-overeenkomst**	Voor de verwerking en opslag van persoonsgegevens en videobeelden, dient Opdrachtnemer met Opdrachtgever een bewerkerovereenkomst af te sluiten.

A15		
BIR 6.1.2	Invulling	Conform sjabloon Opdrachtgever “RWS bewerkersovereenkomst”
B-64 A15	**Spionage**	Opdrachtnemer dient op basis van risicoanalyse maatregelen te treffen om offertes, contracten, netwerkschema’s, constructie, en bouwtekeningen te beveiligen tegen spionage in de breedste zin. *Toelichting intern: nieuwe regelgeving waarop door Veiligheid en Justitie recentelijk binnen RWS een technische kwetsbaarheid onderzoek voor heeft plaatsgevonden.*
	Invulling	Conform richtlijn Opdrachtgever

3 Specifieke maatregelpakketten

De specifieke maatregelpakketten zijn een aanvulling en verdieping op de generieke beheersdoelen en beheersmaatregelen uit hoofdstuk 2. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS volgt om tot beheersing van kwetsbaarheden te komen. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS.

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

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

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

Afhankelijk van de infraclassificatie en het daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maatregelpakketten is gebruik gemaakt van de NCSC Checklist beveiliging ICS/SCADA systemen en overige good practices voor de beveiliging van IA en ICS/SCADA systemen.

Bij mogelijke overlap tussen de generieke beheersdoelen en de specifieke aanvullende maatregelen uit de maatregelpakketten dienen de specifieke aanvullende maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens het bovenliggende generieke beheersdoel en/of beheersmaatregel uit hoofdstuk 2 ingevuld.

3.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten

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

N.B.:

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

Toelichting tabellen

Toegangsbeheer

Rijkspas VG-IA Toegang middels Rijkspas Vitale Gebieden (vanuit IA-perspectief) installatienormen (Grade 3)

Rijkspas Kantoor Toegang middels Rijkspas Kantoor installatienormen

Sleutel Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)

Toegangsproces

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

Organisatorische maatregelen

O1 Standaard maatregelen + voorlichting over preventie + uitleg over het systeem.

O2 Als O1 + specifieke maatregelen opnemen in beveiligingsplan.

Bouwkundige maatregelen

B0 Het aanwezige hang- en sluitwerk handhaven.

B1 Hang- en sluitwerk met een inbraakwerendheid van 3 minuten volgens BRL3104 of klasse 2 NEN5096.

B2 Idem met inbraakwerendheid van 5 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.

B3 Idem met inbraakwerendheid van 10 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.

Compartimentering / Meeneem beperkende maatregelen

C/M1 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M1 door verankeren, verplaatsen. Of bouwkundig compartiment C1. Alles met inbraakvertraging van 3 minuten.

C/M2 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M2 door slagvaste vitrines, rolluiken e.d. Of bouwkundig compartiment C2. Alles met inbraakvertraging van 5 minuten.

C/M3 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M3 door mistgenerator. Of bouwkundig compartiment C3. Alles met inbraakvertraging van 10 minuten.

Elektronische maatregelen

Ed Alleen voor woningen in risicoklasse 1. De (domestic) alarminstallatie met mogelijke doormelding naar (mobiele) telefoon. Grade 2 /NCP 2

E1 Inbraakalarminstallatie. Grade 2 /NCP 2

E2 Inbraakalarminstallatie met ruimtelijk werkende anti-masking detectoren. Grade 2 / NCP 2

E3 Inbraakalarminstallatie met anti-masking detectoren. Componenten Grade 3 /NCP 3

Alarmering

AL0 Optische en/of akoestische alarmgever en/ of alarmtransmissie naar (mobiele) telefoon

AL1 Alarmtransmissiesysteem niveau AL1 volgens NEN EN 50136-1-1 naar een PAC.

AL2 Alarmtransmissiesysteem niveau AL2 volgens NEN EN 50136-1-2 naar een PAC.

AL3 AL2 aangevuld met back-up melding (AL1) via andere transmissieweg (GPRS) naar de PAC.

Reactie (alarmopvolging)

R0 Alarmopvolging door sleutelhouder na melding naar (mobiele) telefoon.

R1 Alarmopvolging door PAC naar de sleutelhouder(s).

R2 Alarmopvolging door PAC naar een erkende Particuliere Bewakingsdienst.

R3 Als R2 + Politie (prioriteit 1) Technische alarmverificatie verplicht.

3.2 Maatregelen Logische toegang

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

Mens	LTM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	LTPO1	Er dient een geborgde procedure te bestaan die de fysieke en logische toegang regelt en een actuele registratie wordt bijgehouden van alle medewerkers inclusief die van onderaannemers voor toegang tot ruimten en informatiesystemen. Tevens dient er voor de lokale logische toegang tot ICT-, ICS/SCADA-systemen en lokale datanetwerken een geborgde procedure en een up-to-date registratie te bestaan van uitgegeven accounts en autorisaties.
	LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend op basis van het ‘need to have’ principe plaatsvindt; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het noodzakelijke; • fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan wordt voor personen die hiertoe geautoriseerd zijn; • bij misbruik van accounts en autorisaties dienen disciplinaire maatregelen te worden genomen.
	LTPO3	De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dient jaarlijks beoordeelt en geactualiseerd te worden in een formeel proces.
	LTPO4	De lokale logische toegang voor medewerkers tot de RWS infrastructuur, ICT, ICS/SCADA systemen en de centrale en locale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager aangevraagd en goedgekeurd te worden.
	LTPO5	De (remote) toegang tot ICT, ICS/SCADA en (ondersteunende) systemen en –objectnetwerken dient altijd en uitsluitend via de centrale, beveiligde en gemonitorde voorzieningen van RWS te verlopen. Hierbij dient gebruik

		te worden gemaakt van de PDC-items van RWS-CIV.
	LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – minimaal een user-id en wachtwoord combinatie met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO7	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – 'two-factor' authenticatie ('bezit' plus 'kennis') met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO8	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – Rijkspas Vitaal ('bezit' plus 'kennis') met navolging van de wachtwoordrichtlijn (indien technisch nog niet mogelijk dan minimaal op basis van user-id en wachtwoord combinatie) • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS/CIV.
	LTPO9	Er dient een geborgde procedure te bestaan die de toewijzing en verspreiding van authenticatiemiddelen aan bedienaars, beheerders en overig ondersteunend personeel regelt alsmede het innemen daarvan bij functiewisseling of vertrek (in-, door- en uitstroming). In deze procedure dient ook de voorgeschreven handelingen bij verlies, diefstal dan wel beschadiging te worden opgenomen.
	LTPO10	De toegang voor onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van dat onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en teruggezet bij afmelding van de call.
Techniek	LTT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.
	LTT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.
	LTT3	Voor bedienaars en beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

3.3 Maatregelen Beveiligingsincidenten en incident Response Plan

Niveau	Mens	Procedures & Organisatie	Techniek
4	BIRM1	BIRPO1 t/m 8	BIRPT1
3	BIRM1	BIRPO1 t/m 8	BIRPT1
2	BIRM1	BIRPO1 t/m 3, 5, 6 en 7	BIRPT1
1	BIRM1	BIRPO1 t/m 3, 5 en 6	BIRPT1

Mens	BIRPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen 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 moet worden geëist dat zij alle beveiligingsincidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.
	BIRPO2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.
	BIRPO3	Er is bestaat een geborgde procedure voor de reactie op en eventuele escalatie van beveiligingsincidenten. De incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, beveiligingsincidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen.
	BIRPO4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op die van RWS-CIV.
	BIRPO5	Er dient een geborgde procedure te bestaan voor de maandelijkse rapportage en evaluatie van alle beveiligingsincidenten, dreigingen en maatregelen die ter zake zijn getroffen.
	BIRPO6	Voor het afhandelen van urgente en niet-standaard beveiligingsincidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incidentmanager van RWS-CIV ingeschakeld.

	BIRPO7	Er dient een geborgde procedure te bestaan voor incidentrespons en continuïteit van de ICT en ICS/SCADA dienstverlening ingeval van incidenten en calamiteiten. De volgende informatie van ICS/SCADA en overige ondersteunende ICT-systemen dient actueel en beschikbaar te zijn voor herstel na een calamiteit: -type en merk ICS/SCADA middel -Formaat -Locatie -Back-up en licenties -Software en hardware configuratie -Vervangingsinstructie/procedure
	BIRPO8	Jaarlijks dienen de ontwikkelde incident responseplannen beproefd te worden aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van incidentresponse is het testen van de noodbediening.
Techniek	BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

3.4 Maatregelen Netwerkkoppelingen

Niveau	Mens	Procedures & Organisatie	Techniek
4	NKM 1	NKPO 1 t/m 9	NKT 1 t/m 3
3	NKM 1	NKPO 1 t/m 9	NKT 1 t/m 3
2	NKM 1	NKPO 1, 2, 4, 5, 6, 7 en 9	NKT 1 t/m 3
1	NKM 1	NKPO 1, 2, 4, 6, 7 en 9	NKT 1 t/m 3

Mens	NKM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	NKPO1	Opdrachtnemer draagt zorg voor en ziet erop toe dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van RWS (zoals vastgelegd in de PDC Netwerken van RWS-CIV) en dat de overige generieke centrale netwerkdiensten evenals overige ondersteunende ICT worden afgestemd en afgenomen van de RWS dienst Centrale Informatievoorziening (CIV). Rechtstreekse toegang tot ICS/SCADA-systemen vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail - is verboden.
	NKPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen het object en de centrale netwerken van RWS (NNV/VicNet) de aansluitvoorwaarden van NNV/VicNet in acht worden genomen. Voor remote logische toegang van personeel tot de aan het object gekoppelde systemen moet de procedure “Toegang Derden” van RWS-CIV worden gevolgd waarbij de Objectverantwoordelijke/-beheer de aanvraag verzorgt.
	NKPO3	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met de RWS-CIV voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de RWS Netwerkarchitectuur inclusief security en de IA-kaderstelling.
	NKPO4	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.
	NKPO5	Opdrachtnemer draagt zorg voor een geborgde procedure die: • alle wijzigingen aan het objectdatanetwerk bijhoudt; • de lokale objectdatanetwerktopologie actueel houdt;

		• een zodanig detailniveau heeft dat alle netwerkkoppelingen en objectdatanetwerkcomponenten met alle relevante informatie beschikbaar is in een Configuration Management Database (CMDB).
	NKPO6	Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen malware, hardening en patching').
	NKPO7	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.
	NKPO8	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door middel van een Configuration Management Database (CMDB).
	NKPO9	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit RWS-CIV.
Techniek	NKT1	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
	NKT2	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.
	NKT3	De besloten (lokale) objectdatanetwerken mogen geen directe internet verbindingen hebben. Dit geldt ook voor draadloze verbindingen (WiFi en GPRS/UMTS, bluetooth etc.) of inbelvoorzieningen.

3.5 Maatregelen bescherming tegen malware, hardening en patching

Niveau	Mens	Procedures & Organisatie	Techniek
4	MHPM 1	MHPPO 1 t/m 11	MHPT 1 t/m 2
3	MHPM 1	MHPPO 1 t/m 11	MHPT 1 t/m 2
2	MHPM 1	MHPPO 1 t/m 5, 7, en 11	MHPT 1 t/m 2
1	MHPM 1	MHPPO 1 t/m 5, 7, en 11	MHPT 1 t/m 2

Mens	MHPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	MHPPO1	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware waarbij de anti-malware software en signature updates dagelijks dienen plaats te vinden.
	MHPPO2	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen door: • niet noodzakelijke datanetwerkservices uit te zetten; • het verwijderen (patchen) van bekende kwetsbaarheden; • alle poorten die niet nodig zijn te deactiveren/blokkeren; • alle default “access points” te verwijderen; • De default accounts uit te schakelen conform het wachtwoord policy; • Indien beschikbaar gebruik te maken van de security opties van leveranciers.
	MHPPO3	Opdrachtnemer draagt zorg voor en ziet erop toe dat removable apparatuur en ICT systemen die gekoppeld worden aan de ICS/SCADA en ondersteunende ICT-systemen en netwerkomgeving waar mogelijk zijn voorzien van alle recente beveiligingsupdates en patches.
	MHPPO4	Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
	MHPPO5	Opdrachtnemer dient over een geborgde procedure te beschikken voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden.
	MHPPO6	Bij patches en anti-virusupdates, die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale

		handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.
	MHPPO7	Opdrachtnemer dient over een geborgde procedure te beschikken die er voor zorgt dat voor kritieke patches binnen 48 uur na melding, gerekend vanaf eerstvolgend werkdag een risicoanalyse wordt uitgevoerd en voorzien is van een implementatieadvies. Voor niet kritieke patches is de doorlooptijd voor uitvoering van risicoanalyse en implementatieadvies maximaal twee maanden. De patches worden na instemming met het implementatieadvies door Opdrachtgever conform het advies door Opdrachtnemer geïmplementeerd.
	MHPPO8	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging schriftelijk te worden vastgelegd voorzien van een risicoafweging.
	MHPPO9	Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
	MHPPO10	Indien haalbaar dienen zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te worden getest.
	MHPPO11	Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op virussen gecontroleerd worden voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
Techniek	MHPT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.
	MHPT2	Antimalware voorzieningen moeten in afstemming met RWS-CIV ingezet worden.

3.6 Maatregelen Logging en Monitoring

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

Mens	LMM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	LMPO1	De handelingen van medewerkers, beheerders, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in audit-logbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf; • een tot een natuurlijk persoon herleidbare gebruikersnaam of een (systeem)-ID • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis • optioneel de identiteit van het werkstation of de locatie • een doorlopende en unieke nummering per logregel
	LMPO2	Opdrachtnemer draagt zorg voor en ziet er op toe dat: • de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden een maand bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
	LMPO3	Voor de levering van logbestanden aan derden dient de RWS Objectverantwoordelijke/-beheerder expliciet toestemming te verlenen.
	LMPO4	Opdrachtnemer draagt zorg voor een geborgde procedure die opvolging geeft aan meldingen uit de centrale logging en monitoringsvoorzieningen en proces vanuit RWS-CIV.
	LMPO5	Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het ICS/SCADA en gekoppelde ICT-componenten in kaart gebracht. Een geborgde procedure is aanwezig voor het bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.

Techniek	LMT1	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en- netwerkelementen dienen in CSV-formaat opgeleverd te kunnen worden.
	LMT2	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.
	LMT3	Het overschrijven of verwijderen van logregels- en bestanden wordt gelogd in een nieuw aangelegde log.
	LMT4	De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.
	LMT5	Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen moet in afstemming met en op verzoek van Opdrachtgever beveiligingsspecifieke logsystemen worden ingezet.

3.7 Maatregelen Bewustwording en Training

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

Medewerker	BTME1	Bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door het management aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen.
	BTME2	Iedere medewerker is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.
	BTME3	Bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
	BTME4	Bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.
	BTME5	Bij het constateren van een beveiligingsincident dienen bedienaars, beheerders en overig ondersteunend personeel dit direct als een beveiligingsincident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een beveiligingsincident bij het manifest worden van een (dreigend of reeds opgetreden) beveiligingsrisico als gevolg van een (mogelijke) overtreding van het beveiligingsbeleid of onregelmatigheid. Voorbeelden van beveiligingsincidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen;

		- niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
	BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.
	BTME7	Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
	BTME8	Bedienaars, beheerders en overig ondersteunend personeel gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
	BTME9	Bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
	BTME10	Bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.
	BTME11	Bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele viruscontrole van apparatuur/media mogen doen.
	BTME12	Voor bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
	BTME13	Bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
	BTME14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar

		de voor dat account geautoriseerde persoon.
	BTME15	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 wijzigen conform de wachtwoordrichtlijn van RWS.
	BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
	BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
	BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.
	BTME19	Gegevensdragers worden altijd vooraf op virussen gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
	BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME22	Bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.
Manager	BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
	BTMA2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: • de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel, objectverantwoordelijke/-beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; • ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; • dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen alle

		bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van RWS die ze in hun bezit hebben retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; • dat de toegangsrechten van alle bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.
	BTMA3	De objectverantwoordelijke/-beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.
	BTMA4	Opdrachtnemer ziet erop toe dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging zoals fysieke en logische toegang en melding van beveiligingsincidenten. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steeksproefsgewijze controles vastgesteld en uitgevoerd.
	BTMA5	Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
	BTMA6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.

3.8 Maatregelen gecontroleerd wijzigen

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

Mens	GWM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	GWPO1	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) inventariseren en registreren van alle Configuration Items (CI’s) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden.
	GWPO2	Opdrachtnemer dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd.
	GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.
	GWPO4	Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen dient altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten voordat uitvoering van werkzaamheden plaatsvindt zijn goedgekeurd door de Objectverantwoordelijke/ -beheerder.
	GWPO5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.
	GWPO6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten indien mogelijk vooraf aan de implementatie in productie te worden getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit of beveiliging van de organisatie. Indien haalbaar moet voor ICS/SCADA en overige ondersteunende ICT-systemen controle worden uitgevoerd voor de authenticiteit/integriteit van de software voorafgaande aan de implementatie op operationele systemen.

	GWPO7	Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebrachte als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.
	GWPO8	Voor elke wijziging is een terugval scenario opgesteld waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. Kort na de implementatie van een wijziging dient een test plaats te vinden om te verifiëren dat de wijziging is gelukt of dat op het terugval scenario moet worden overgegaan.
	GWPO9	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.
Techniek	GWT1	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.
	GWT2	Voor zover beschikbaar wordt gebruik gemaakt van testvoorzieningen.

3.9 Maatregelen beheer en onderhoud

Niveau	Mens	Procedures & Organisatie	Techniek
4	BOM 1	BOPO 1 t/m 9	BOT 1 t/m 2
3	BOM 1	BOPO 1 t/m 9	BOT 1 t/m 2
2	BOM 1	BOPO 1 t/m 4, 6 en 9	BOT 1 t/m 2
1	BOM 1	BOPO 1 t/m 4, 6	BOT 1 t/m 2

Mens	BOM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset “bewustwording en training”.
Procedures & Organisatie	BOPO1	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.
	BOPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers: • Geheimhouding opgenomen is; • Training- en opleidingsvereisten alsmede overige benodigde certificeringen beschreven zijn; • Welke screening van personeel nodig is (bijv. VOG); • Beschreven is dat de RWS gedragsregels voor beveiliging en communicatie strikt in acht moeten worden genomen; • Een concrete procedure bekend is en is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) • De procedures voor fysieke toegang tot objecten en ruimten en de logische toegang tot systemen vastgelegd zijn; • De registratie en rapportage van beveiligingsincidenten geregeld is; • Beschreven is dat handelingen van medewerkers en systemen gelogd en gemonitord worden; • Beschreven is dat loggegevens van RWS beschermd moeten worden tegen verlies en wijziging en niet voor andere doeleinden gebruikt mogen worden; • De bewaartermijnen van back-ups en logbestanden geregeld is; • De procedures voor aan- en afkoppeling van apparatuur beschreven zijn; • De netwerkaansluitvoorwaarden overeengekomen zijn; • De procedure “Toegang Derden” van de CIV gevolgd moet worden voor de logische toegang tot netwerken en systemen. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. • Beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die voorzien zijn van de laatste security update’s en patches en actuele viruscontroleprogrammatuur; • Beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van RWS verlopen;

		• Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van RWS; • Beschreven is dat wijzigingen conform het wijzigingsproces van RWS uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden van RWS uitgevoerd moeten worden; • Beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; • Beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het RWS of objectnetwerken strikt verboden is.
	BOPO3	Opdrachtnemer draagt waar nodig zorg voor en ziet erop toe dat in de SLA/DAP afspraken met Opdrachtgever en onderaannemers worden gemaakt over: • De dienstverlening en functionaliteit; • Tijd van openstelling, bereikbaarheid en reactietijd, incident melding en afhandeling; • Wat wordt verstaan onder een storing, beveiligingsincident en zwakke plek; • Het classificeren van incidenten en de geldende maximale oplossingsduur; • Escalatieprocedures (horizontaal en verticaal) bij overschrijding van de overeengekomen normtijden inclusief namen en telefoonnummers. • Het indienen en afhandelen van wijzigingsverzoeken; • Directe melding van beveiligingsincidenten; • Noodprocedures met zowel interne als externe leveranciers voor ICT en ICS/SCADA systemen; • Ondersteuning bij calamiteiten en beschikbaarheid van reserve onderdelen en apparatuur; • De communicatielijnen (wie, wanneer en waarover); • Hoe de fysieke en logische toegang tot systemen en ruimten geregeld is; • De bewaartermijn van back-ups en logbestanden; • Rapportages die verplicht zijn zoals die voor beveiligingsincidenten en welke frequentie daarvoor geldt; • Het signaleren van nieuwe kwetsbaarheden en tijdig uitbrengen van patches door de leverancier; • Het testen van software-updates alvorens deze in productie gaan; • Evaluatie en actualisatie;
	BOPO4	Opdrachtnemer draagt zorg voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
	BOPO5	Opdrachtnemer draagt zorg voor een geborgde procedure die de personele toegang van al het vast onderhoudspersoneel voorafgaand de uitvoering van werkzaamheden regelt. Hiervoor kan de onderstaande “Good Practice” “**Maatregelen personele toegang**” gebruikt worden.
	BOPO6	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: • de uitvoering van wijzigingen conform de wijzigingen procedure; • de procedure voor fysieke toegang; • de procedure voor logische toegang; • patching, de back-up procedure en bewaartermijnen; • incidentmanagement, log- en incidentrapportages en de analyse

		hiervan.
	BOPO7	Opdrachtnemer draagt zorg voor een geborgde procedure voor incidentrespons en continuïteit van de ICT en ICS/SCADA dienstverlening ingeval van incidenten en calamiteiten. De volgende informatie van ICS/SCADA en overige ondersteunende ICT-systemen dient actueel en beschikbaar te zijn voor herstel na een calamiteit: -type en merk ICS/SCADA middel -Formaat -Locatie -Back-up en licenties -Software en hardware configuratie -Vervangingsinstructie/procedure
	BOPO8	Opdrachtnemer draagt zorg voor en ziet erop toe dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.
	BOPO9	Opdrachtnemer dient jaarlijks de opzet, bestaan en werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever.
Techniek	BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.
	BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV.

Good Practice - Maatregelen personele toegang

De Opdrachtnemer dient te verzorgen dat al het vast onderhoudspersoneel voorafgaand aan zijn/haar operationele inzet en vervolgens steeds binnen een

periode van twee jaar:

- een persoonlijke geheimhoudingsverklaring ondertekent en overhandigt aan de Opdrachtgever;

- zich daarbij legitimeert en een goed gelijkende pasfoto overhandigt aan de Opdrachtgever;

- een Verklaring Omtrent Gedrag (VOG) bezit en een kopie daarvan aan de Opdrachtgever overlegt welke is gerelateerd aan de beoogde Werkzaamheden.

Hangende de aanvraag voor een VOG kan volstaan worden met een eigen verklaring van de betreffende medewerker gedurende een periode van maximaal zes weken

welke niet verlengd kan worden.

De Opdrachtnemer dient er op toe te zien dat al het onderhoudspersoneel dat niet structureel verschijnt:

- Zich legitimeert;

- In specifieke gevallen op eerste verzoek van de Opdrachtgever bereid is een eigen verklaring en een geheimhoudingsovereenkomst te ondertekenen.

De Opdrachtnemer dient al haar medewerkers nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.

Iedere geconstateerde afwijking van bovenstaande eisen dient door de Opdrachtnemer te worden behandeld als security incident.

3.10 Maatregelen Back-ups

Niveau	Mens	Procedures & Organisatie	Techniek
4	BUM 1	BUPO 1 t/m 5	BUT 1
3	BUM 1	BUPO 1 t/m 5	BUT 1
2	BUM 1	BUPO 1 t/m 5	BUT 1
1	BUM 1	BUPO 1 t/m 3	BUT 1

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

		maatregelen getroffen.
Techniek	BUT1	Benodigde voorzieningen voor het back-up en restoreproces worden in overleg met de Opdrachtgever ingevuld.

Bijlage A: Wachtwoord Richtlijn

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

De eisen aan een wachtwoord zijn als volgt:

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

Voor de hieronder genoemde accounttypen dient de standaard fabrieksaccount met bijbehorend wachtwoord altijd gewijzigd te worden door een persoonlijk account en wachtwoord. Tevens dient voor de onderkende accounttypen de aangegeven duur voor wachtwoordvervanging alsmede de wachtwoordlengte aangehouden te worden. Bij (legacy) systemen en procestoepassingen waar dit niet mogelijk is, moet een risico-inschatting worden gemaakt en compenserende maatregelen worden getroffen. De afwijkingen worden gedocumenteerd.

De voorschriften rondom accounts en wachtwoorden voor kantoorautomatiseringstoepassingen zijn ter verkrijgen bij de afdeling IV - Security Center van RWS-CIV.

Onderkend worden de volgende typen accounts voor ICS/SCADA met bijbehorende eisen:

Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT-producten van fabrikanten worden gewijzigd.

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

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

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

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

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

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

Bijlage B: Factsheet Wachtwoorden

Factsheet wachtwoorden voor gebruikers van IA systemen

Aanleiding

Steeds meer Industriële Automatiseringssystemen worden aan andere computersystemen of netwerken gekoppeld. Daarmee neemt de kans toe dat deze systemen vanaf een andere computer of netwerk worden gehackt, met mogelijk verstrekkende gevolgen.

Door het handhaven van fabriekswachtwoorden of eenvoudig te kraken wachtwoorden op IA systemen kunnen kunstwerken en verkeerssystemen relatief eenvoudig worden overgenomen door hackers, als ze via internet of fysiek toegang kunnen krijgen tot de IA systemen.

Toepassing factsheet

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

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

Checklist eigenschappen sterke wachtwoorden

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

Zwakke wachtwoorden hebben de volgende eigenschappen:

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

Tips voor het maken en onthouden van sterke wachtwoorden

- maak een wachtwoord dat is gebaseerd op een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (Bijvoorbeeld: Het rijmpje “Als het regent in mei is april voorbij en leggen alle vogels een ei” wordt “Ahri5i4velavee”, waarbij de maanden zijn vervangen door cijfers)
- maak een zin (passphrase) in plaats van een wachtwoord (password). Typ de woorden van een makkelijke zin achterelkaar en vervang woorden of letters door hoofdletters, getallen of lettertekens (Bijvoorbeeld: 03KleineKleutertjesdiezatenopeen###).

Checklist wachtwoordbescherming

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

Slechte opslag van wachtwoorden voldoet aan de volgende eigenschappen:

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

Tips voor het opslaan van wachtwoorden

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

Checklist wachtwoordwijziging

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

Tips voor het wijzigen van wachtwoorden

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

Checklist locken bedien- of beheerstation

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

Tips voor het locken van bedien- of beheerstation

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

Bijlage 1 Gebruikersmaatregelen

Risicoreductieoverzicht logische toegang IA bediening en beheer vanuit gebruikersperspectief