Stappenplan implementatie BIO IA voor decentrale overheden

Handreiking voor gemeenten en provincies om te voldoen aan de Baseline Informatiebeveiliging Overheid voor Industriële automatisering

kennisplatform CROW

CROW is een onafhankelijke kennisorganisatie zonder winstoogmerk die investeert in kennis voor nu en in de toekomst. Wij streven naar de beste oplossingen voor vraagstukken van beleid tot en met beheer in infrastructuur, openbare ruimte, verkeer en vervoer en werk en veiligheid. Bovendien zijn wij experts op het gebied van aanbesteden en contracteren.
Meer informatie: crow.nl

landelijk programma iCentrale

In het landelijke programma iCentrale hebben marktpartijen en decentrale overheden gezamenl ijk diensten ontwikkeld op het gebied van verkeersmanagement, parkeermanagement en -beheer, brug- en sluisbediening, tunnelbewaking en -bediening, stadstoezicht en -beheer en crowd- en event-management. Dit hebben zij gedaan onder de (communicatie) vlag van iCentrale.nl, iDiensten.nl en MaaSandMore.com.
Meer informatie: iCentrale.nl

Ministerie van Infrastructuur en Waterstaat

Het programma iCentrale is mede mogelijk gemaakt door het ministerie van Infrastructuur en Waterstaat (IenW), DG Mobiliteit. IenW zet in op leefbaarheid en bereikbaarheid, met een vlotte doorstroming in een goed ingerichte, schone en veilige omgeving.
Meer informatie:minienw.nl

Woord vooraf

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vindt haar oorsprong in de kantoorautomatisering (KA). Overheden maken voor het kosteneffectief realiseren van hun beleidsdoelen steeds vaker ook gebruik van industriële automatisering (IA). Van IA is sprake als objecten in de openbare ruimte worden verbonden ("connected" gemaakt) en onderdeel worden van het Internet of Things (IoT). Dit wordt gedaan om objecten op afstand te kunnen monitoren, bewaken, beheren, aansturen en/of bedienen. Voorbeelden van deze objecten zijn bruggen, sluizen, tunnels, verkeersmanagementsystemen zoals intelligente verkeersregelinstallaties (iVRI's) en objecten voor stadszicht- en beheer zoals camera's en verdwijnpalen (pollers).

De iDiensten die binnen het landelijk programma iCentrale zijn ontwikkeld en beproefd, zijn gericht op het op afstand monitoren, bewaken, beheren, aansturen en bedienen van meerdere objecten in meerdere domeinen die in eigendom zijn van overheden. Door het gebruiken van iDiensten kunnen overheden hun objecten tegen lage(re) kosten laten bedienen en hiermee hoge(re) baten behalen (netwerkprestaties en maatschappelijke baten). Voor de iDiensten zijn landelijke specificaties opgesteld die worden gebruikt om middels een landelijke aanbesteding te komen tot een landelijke Menukaart iDiensten. In de specificaties voor de iDiensten is de BIO zodanig opgenomen, dat elke iDienst die door een aanbieder wordt aangeboden voldoet aan de BIO. Daarmee is gewaarborgd dat het private deel van deze publiek-private keten voldoet aan de wettelijke eisen t.a.v. cybersecurity.

De BIO heeft betrekking op de gehele (publiek-private) keten, dus ook op de overheidsorganisaties en hun medewerkers zelf en de instrumenten (zoals eigen bedien-, beheer- en verkeerscentrales) en middelen die zij hiervoor zelf gebruiken. De meeste overheden zijn zich bewust van deze opgave, maar worstelen met de implementatie van de cybersecuritymaatregelen in de IA om aantoonbaar aan het nieuwe wettelijke normenkader van de BIO te voldoen. Deze opgave is er vanzelfsprekend ook als de gehele bedienketen publiek wordt uitgevoerd.

RWS heeft op het gebied van informatiebeveiliging voor industriële automatisering met de CyberSecurity Implementatie Richtlijn (CSIR) een praktische invulling van de BIO voor IA uitgewerkt en past deze al jaren in de praktijk toe. Deze aanpak is generiek van opzet en daardoor ook bruikbaar voor andere overheden, en vormt dan ook een integraal onderdeel van deze standaard (deel B). Om de cybersecurity IA aanpak van RWS ook toepasbaar en praktisch werkbaar te maken voor gemeenten en provincies is de voorliggende handreiking gemaakt. Met deze handreiking kan een gemeente of provincie in 10 relatief eenvoudige stappen in beeld brengen en toepassen wat er nodig is te verzorgen dat de eigen organisatie, medewerkers en instrumenten en middelen gaan voldoen aan de BIO voor IA.

Wij danken alle deskundigen vanuit private partijen en overheden die hebben bijgedragen aan de totstandkoming van het "Stappenplan implementatie BIO IA voor decentrale overheden".

Pieter Litjens, directeur-bestuurder CROW
Jan-Bert Dijkstra, directeur programma Mobiliteit en Gebieden, Ministerie van Infrastructuur en Waterstaat
Lindy Molenkamp, directeur beheer en uitvoering, penvoerder programma iCentrale, Provincie Noord-Holland

De brochure kwam tot stand dankzij medewerking van:

Schrijvers

Paul Oost, KienIA Industriële Automatisering B.V.
Gijs Withagen, KienIA Industriële Automatisering B.V.
Eelco Banis, KienIA Industriële Automatisering B.V.

Reviewers/genodigden workshop

Ron Perrier, ENGIE Infra & Mobility B.V.
Mark van Leeuwen, Rijkswaterstaat
Jan Jaap van Dijke, Provincie Utrecht
Theo Sikkema, Provincie Overijssel
Puck van Liere, Provincie Overijssel
Nico van Beugen, Gemeente Deventer
Robert Kooijman, Gemeente Rotterdam
Tino van As, Infra-knowledge
Paul Zunderdorp, Provincie Noord-Holland
Corné van Iersel, Nedmobiel B.V.
Hillie Talens, CROW, expert, coördinator landelijke standaards CROW
Marcel Westerman, MARCEL, Adviseur Proposities programma iCentrale
Gerard Martens, Martens Verkeersadvies, adviseur Programma van Eisen, programma iCentrale
André Loos, Landelijk programmamanager programma iCentrale

Inhoudsopgave

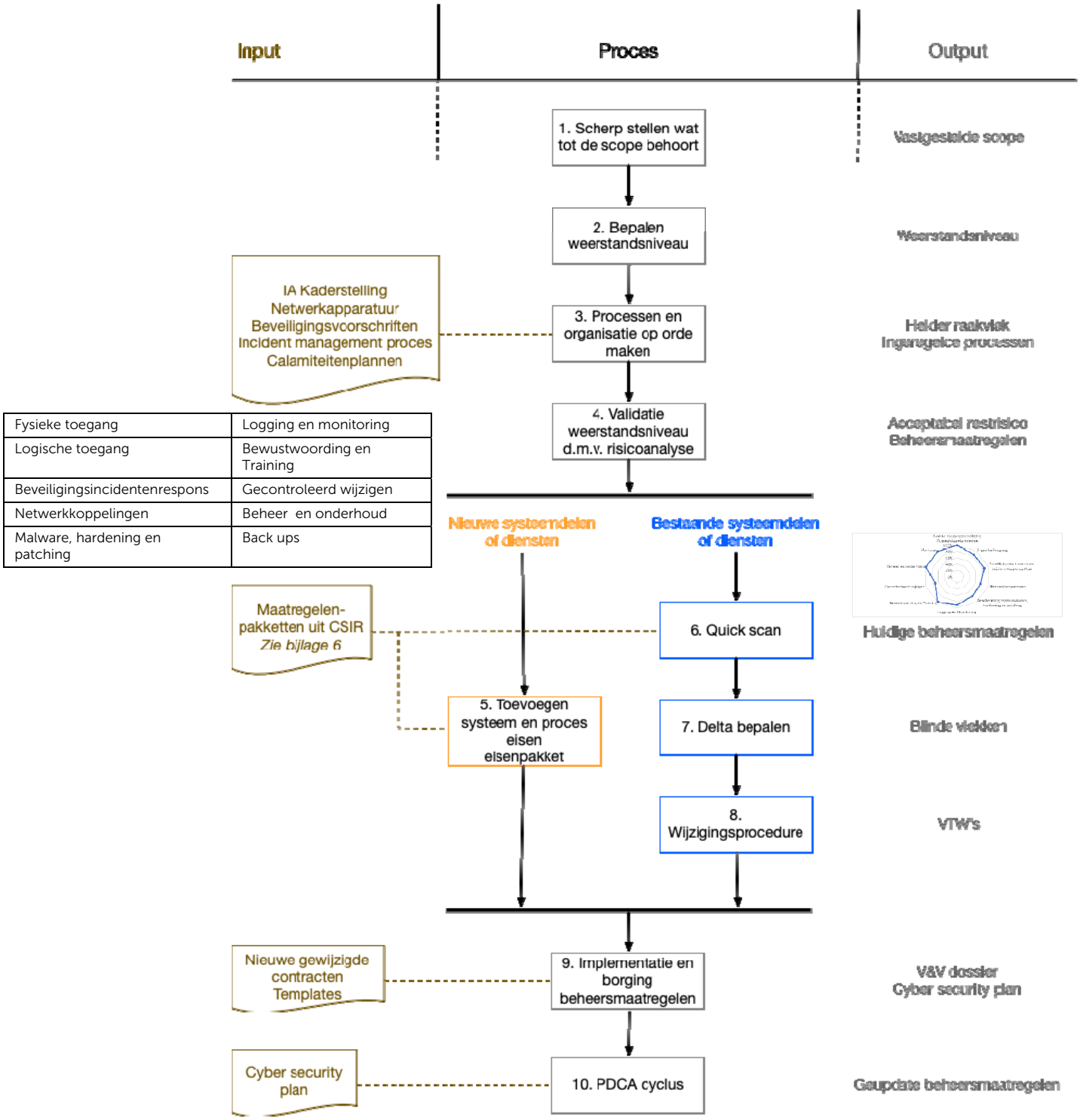
Managementsamenvatting

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vindt haar oorsprong in de kantoorautomatisering (KA). Overheden maken voor het kosteneffectief realiseren van hun beleidsdoelen steeds vaker ook gebruik van industriële automatisering (IA). Van IA is sprake als objecten in de openbare ruimte worden verbonden ("connected" gemaakt) en onderdeel worden van het Internet of Things (IoT). Dit wordt gedaan om objecten op afstand te kunnen monitoren, bewaken, beheren, aansturen en/of bedienen. Voorbeelden van deze objecten zijn bruggen, sluizen, tunnels, verkeersmanagementsystemen zoals intelligente verkeersregelinstallaties (iVRI's) en objecten voor stadszicht- en beheer zoals camera's en verdwijnpalen (pollers).

De iDiensten die binnen het programma iCentrale zijn ontwikkeld en beproefd, zijn gericht op het op afstand monitoren, bewaken, beheren, aansturen en bedienen van meerdere objecten in meerdere domeinen die in eigendom zijn van overheden. Door het gebruiken van iDiensten kunnen overheden hun objecten tegen lage(re) kosten laten bedienen en hiermee hoge(re) baten behalen (netwerkprestaties en maatschappelijke baten). Voor de iDiensten zijn landelijke specificaties opgesteld die worden gebruikt om middels een landelijke aanbesteding te komen tot een landelijke Menukaart iDiensten. In de specificaties voor de iDiensten is de BIO zodanig opgenomen, dat elke iDienst die door een aanbieder wordt aangeboden voldoet aan de BIO. Daarmee is gewaarborgd dat het private deel van deze publiek-private keten voldoet aan de wettelijke eisen t.a.v. cybersecurity.

De BIO heeft betrekking op de gehele (publiek-private) keten, dus ook op de overheidsorganisaties en hun medewerkers zelf en de instrumenten (zoals eigen bedien-, beheer- en verkeerscentrales) en middelen die zij hiervoor zelf gebruiken. De meeste overheden zijn zich bewust van deze opgave, maar worstelen met de implementatie van de cybersecurity maatregelen in de IA om aantoonbaar aan het nieuwe wettelijke normenkader van de BIO te voldoen. Deze opgave is er vanzelfsprekend ook als de gehele bedienketen publiek wordt uitgevoerd.

RWS heeft op het gebied van informatiebeveiliging voor industriële automatisering met de CyberSecurity Implementatie Richtlijn (CSIR) een praktische invulling van de BIO voor IA uitgewerkt en past deze al jaren in de praktijk toe. Deze aanpak is generiek van opzet en daardoor ook bruikbaar voor andere overheden. Om de cybersecurity IA aanpak van RWS ook toepasbaar en praktisch werkbaar te maken voor gemeenten en provincies is de voorliggende handreiking gemaakt. Met deze handreiking kan een gemeente of provincie in 10 relatief eenvoudige stappen in beeld brengen en toepassen wat er nodig is te verzorgen dat de eigen organisatie, medewerkers en instrumenten en middelen gaan voldoen aan de BIO voor IA.



Fysieke toegang	Logging en monitoring
Logische toegang	Bewustwoording en Training
Beveiligingsincidentenrespons	Gecontroleerd wijzigen
Netwerkkoppelingen	Beheer en onderhoud
Malware, hardening en patching	Back ups

Deel A

Stappenplan implementatie BIO IA voor decentrale overheden

Handreiking voor gemeenten en provincies om te voldoen aan de Baseline Informatiebeveiliging Overheid voor Industriële automatisering

1 Achtergrond van deze leidraad

Overheidsinstanties maken voor het behalen van hun bedrijfsdoelen gebruik van industriële automatisering (IA). IA omvat computers die installaties aansturen, de bedien- en bewaakstations, informatiesystemen die alles loggen en managementsystemen die de functionaliteit, productie en het onderhoud coördineren. Voorbeeld hiervan zijn installaties zoals bruggen- en sluizen, waterzuiveringen en tunnels, maar ook controlekamers van waaruit vele installaties worden bediend en bewaakt.

Tegenwoordig worden installaties steeds meer integraal op elkaar aangesloten om optimaal samen te werken. Het concept van de iCentrale en iDiensten zijn daar een goed voorbeeld van. Communicatie en informatie-uitwisseling loopt via het internet of via andere netwerken, waarbij de informatiedeling leidt tot snelle optimalisatieslagen en flexibele productie.

Het doel van deze publicatie is om een praktisch hanteerbare leidraad te geven zodat decentrale overheden (DCO's), op basis van generieke wetgeving en bestaande best practices enerzijds, en de eigen bedrijfsdoel-stellingen anderzijds, komen tot een securitybeleid. Om dit vervolgens te vertalen naar praktisch implementeer-bare maatregelen voor de industriële automatisering.

Cyberdreiging neemt toe

Het belang van informatiebeveiliging neemt hierdoor ook sterk toe, omdat functionaliteit, productie en onder-houd niet meer zonder informatie-uitwisseling kunnen. Het Nationaal Cybersecuritycentrum (NCSC) heeft vastgesteld dat cyberdreigingen permanent van karakter zijn en waarschuwt voor spionage, verstoring en sabotage.

''Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland. De afhankelijkheid van gedigitaliseerde processen en systemen is zo groot geworden dat aantasting kan leiden tot maatschappij-ontwrichtende schade.'' (Cybersecuritybeeld Nederland, 2019). De impact van een verstoring van vitale systemen is recent nogmaals duidelijk geworden met de storing bij KPN (juni 2019) en daardoor de onbereikbaarheid van het landelijke alarmnummer. Dit toont nogmaals de afhankelijkheid van zulke vitale systemen aan.

Ook industriële automatiseringssystemen lopen gevaar. Daarom verdient Cybersecurity de aandacht. Met de juiste aanpak en het nemen van gerichte maatregelen zijn de risico's van een cyberaanval goed te beheersen. Op die manier wordt voorkomen dat uw productie stilvalt of dat er andere schade ontstaat.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) adviseert burgers, bedrijven en overheid om de weerbaarheid tegen cyberaanvallen te vergroten om risico's te verminderen. Wereldwijd, ook in Nederland, lopen er programma's om de weerbaarheid van de vitale infrastructuur te verbeteren.

Overheden gaan over op de BIO

Informatiebeveiliging maakt op dit moment al onderdeel uit van processen en systemen bij de overheids-organisaties. Zij hebben beheersmaatregelen geïmplementeerd, die van toepassing zijn op mensen, processen of systemen.

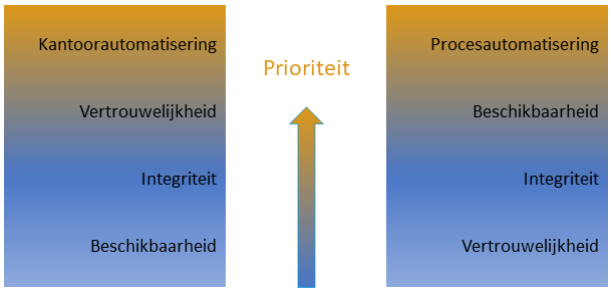
Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO heeft als doel de informatie(-systemen) bij alle overheidsinstanties te beschermen. Alle lagen van de overheid dienen erop toe te zien dat onderling uitgewisselde gegevens beveiligd en in overeenkomst zijn met wet- en regelgeving. De BIO geldt voor alle overheidsinstanties en vervangt de huidige verschillende baselines informatieveiligheid van Gemeenten, Rijk, Waterschappen en Provincies (IBI, BIG, BIR, BIWA) die gebaseerd zijn op oudere versie van de NEN-ISO 27001-norm (2005 en 2013). De gehele overheid standaardiseert hiermee de aanpak van haar beveiligingsbeleid.

De nieuwe BIO is gebaseerd op de NEN-ISO 27001:2017. Door het gezamenlijk gebruik van de BIO ontstaat één normenkader. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. Door de BIO weet straks elke overheidsinstantie dat de gegevens die verstuurd worden naar een ander organisatie-onderdeel of andere overheidsinstantie op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

BIO in relatie tot Industriële Automatisering

Ook in het werkveld industriële automatisering (IA) moet de informatiebeveiliging conform de BIO worden ingericht. Om te voldoen aan de BIO moeten overheden beheersmaatregelen implementeren in de IA-keten. Veel overheden worstelen met de implementatie van de maatregelen in de IA om aantoonbaar aan het nieuwe normenkader te voldoen. Een van de oorzaken hiervoor is dat de BIO haar oorsprong vindt in de kantoorautomatisering (KA) en daarmee niet altijd goed toepasbaar is binnen de systeemcontext van een industrieel automatiseringssysteem.

Het klassieke verschil tussen IA en KA ligt in het verschillend omgaan met de aspecten beschikbaarheid, vertrouwelijkheid en integriteit. Bij KA is over het algemeen vertrouwelijkheid het belangrijkste aspect en bij IA ligt de hoogste prioriteit bij beschikbaarheid.



Figuur 1 Verschil in prioritering KA en IA / procesautomatisering

Wanneer bijvoorbeeld in een provincie de informatie op welk exacte tijdstip een brug open is geweest 8 uur lang niet beschikbaar is, wordt het primaire proces niet gehinderd en kan verkeer gewoon doorgang vinden. Wanneer de brug echter een halve dag niet bediend kan worden wanneer er een schip aankomt, wordt het primaire proces wel gehinderd. De provincie en belanghebbenden lijden hierdoor direct schade. De schade kan zelfs nog groter zijn, wanneer door een cyberincident tijdens het draaien van een brug het systeem wordt gesaboteerd.

Beschikbaarheid heeft hier de hoogste prioriteit. In tegenstelling tot de kantoorautomatisering, waar bijvoorbeeld een kostprijsberekening van een aan te bieden dienst zeer waardevol is en beschermd dient te worden, maar als het een half dag duurt om dat te herstellen na een systeemcrash, dan is het leed meestal te overzien. *Vertrouwelijkheid* is hier meer van belang.

Omdat de prioritering in de werkvelden anders is, zullen ook de beheersmaatregelen met betrekking tot IA en KA verschillen.

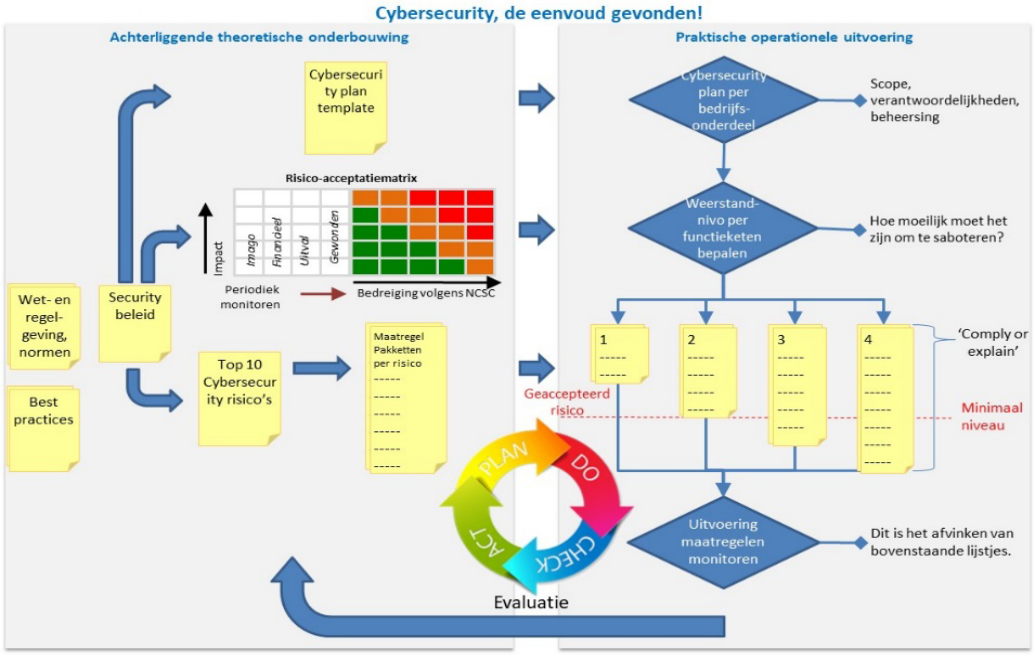
Dit betekent overigens niet dat integriteit en vertrouwelijkheid voor de IA niet relevant zijn. Zo is de integriteit van een brugstatussignaal essentieel om een brug veilig te kunnen bedienen. En het beschermen van de vertrouwelijkheid van kentekens die in worden gewonnen in een reistijdmeetsysteem is zeker een aspect dat ook aandacht verdiend.

2 Van beleid naar maatregelen

De uitdaging waarvoor de overheidsorganisaties staan is hoe de kaders uit de BIO te vertalen naar een passende invulling in de IA praktijk. Hoe vertalen wetgeving, beleid, normen en richtlijnen zich naar een passende bescherming van de IA assets en daarmee een beheersing van de bedrijfsrisico's?

In figuur 2 is dit schematisch weergegeven. Aan de linkerzijde van de figuur is uitgewerkt hoe vanuit beleid, doelstellingen en risico analyse gekomen wordt tot de te implementeren maatregelen. Hier zit het denkwerk, de afstemming en afweging, en de besluitvorming.

De plannen en maatregelenpakketten die hieruit voortkomen kunnen daarna door de assetbeheerders worden uitgevoerd of in opdracht gegeven worden bij opdrachtnemers.



Figuur 2 Risico-gestuurde methode om aan alle normen, eisen en beleid rond cybersecurity invulling te geven en te vertalen naar uitvoerbare maatregelen in de praktijk.

Door op reguliere basis de effectiviteit van de maatregelen te evalueren ten opzichte van de beheersdoelen wordt de Deming cirkel (PDCA) gesloten. In de evaluatieslag wordt bovendien beschouwd of naar aanleiding van wijzigende omstandigheden de beheersdoelen moeten worden bijgesteld.

Deze manier van denken heeft ten grondslag gelegen aan de ontwikkeling van de CyberSecurity Implementatierichtlijn Objecten Rijkswaterstaat (CSIR). DCO's kunnen hier gebruik van maken. Hoe? dat wordt in de volgende hoofdstukken uitgewerkt.

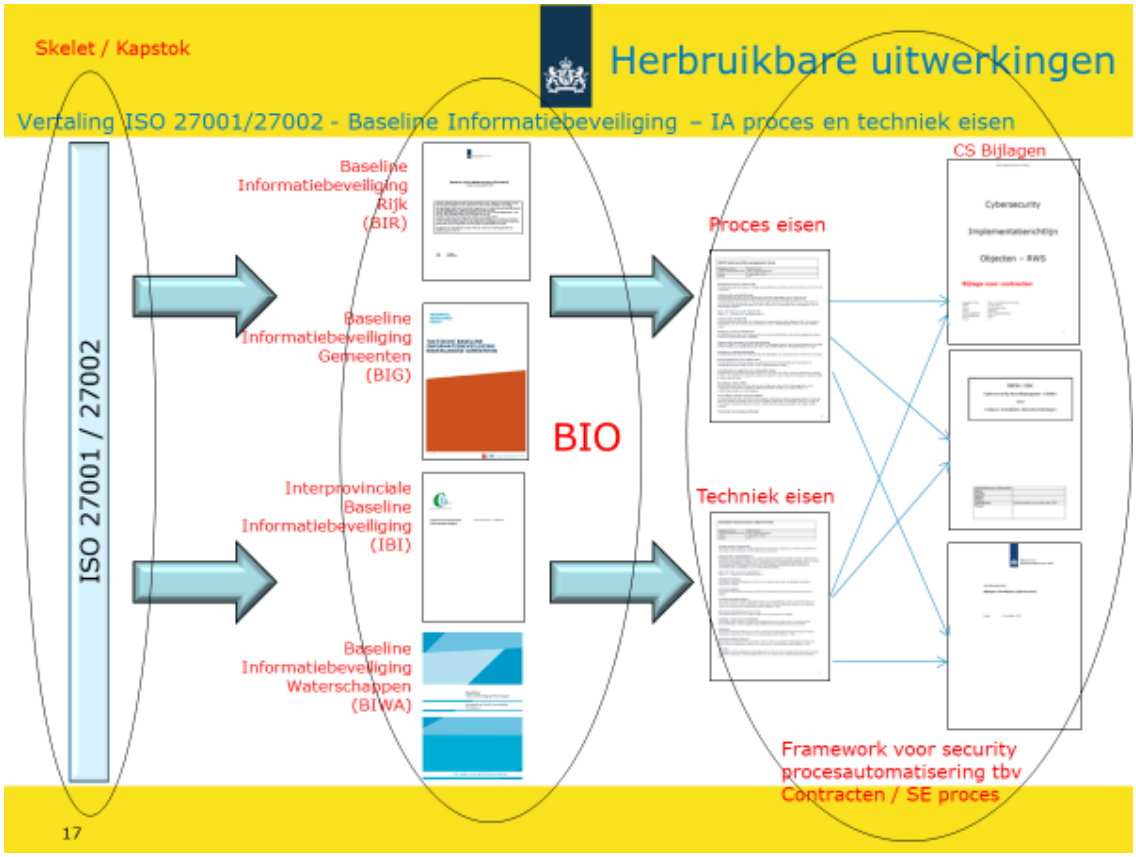
3 Toepassing CSIR binnen DCO

3.1 Wat houdt de CSIR van Rijkswaterstaat in

Rijkswaterstaat (RWS) heeft met de CyberSecurity Implementatierichtlijn Objecten Rijkswaterstaat (CSIR) een praktische risico-gestuurde aanpak ontwikkeld. De aanpak is toegespitst op informatiebeveiliging in de industriële techniek en heeft al sinds 2013 zijn kwaliteit bewezen.

In dit hoofdstuk wordt uitgewerkt hoe deze RWS methode ingezet kan worden door DCO's die iDiensten gaan implementeren. Een van de redenen om deze methode van RWS te omarmen is dat RWS zelf ook bezig is met de waterschappen om onder de vlag van de NCSA (Nationale CyberSecurity Agenda) haar methode breder toepasbaar te maken (Kamerbrief Beleidsreactie CSBN2019 en voortgangsrapportage NCSA, 12 juni 2019).

De aanpak van RWS is beschreven in een aantal documenten en templates. Deze zijn opgenomen in de bijlagen (1 t/m 4).



Figuur 3 RWS aanpak van BIO naar praktische invulling.

Het bovenstaande figuur geeft weer hoe RWS de ISO27001/27002 door laat werken in de BIO en hoe de BIO vervolgens doorwerkt in projecten door middel van techniek- /systeemeisen en proces- /managementeisen (zie figuur 3).

In bijlage 1 en 2 zijn de systeem- en managementeisen opgenomen zoals die door RWS worden opgenomen in contracten richting haar opdrachtnemers. Bijlage 1 is specifiek ontwikkeld voor natte projecten, maar is even-eens toepasbaar op droge projecten en iDiensten. Deze eisen zijn geformuleerd in de vorm van beheersdoelen. Vanuit deze eisen wordt verwezen naar maatregelpakketten en te hanteren richtlijnen zoals opgenomen in bijlage 3 en 4.

Deze maatregelenpakketten zijn gecategoriseerd naar de volgende aandachtsgebieden. Per aandachtsgebied is steeds aangegeven welke maatregelen van toepassing zijn voor een bepaald weerstandsniveau:

Gebieden	
1.	Fysieke toegangsbeveiliging IA-gerelateerde ruimten
2.	Logische toegang
3.	Beveiligingsincidenten en incident Response Plan
4.	Netwerkkoppelingen
5.	Bescherming tegen malware, hardening en patching
6.	Logging en Monitoring
7.	Bewustwording en Training
8.	Gecontroleerd wijzigen
9.	Beheer en onderhoud
10.	Back-ups

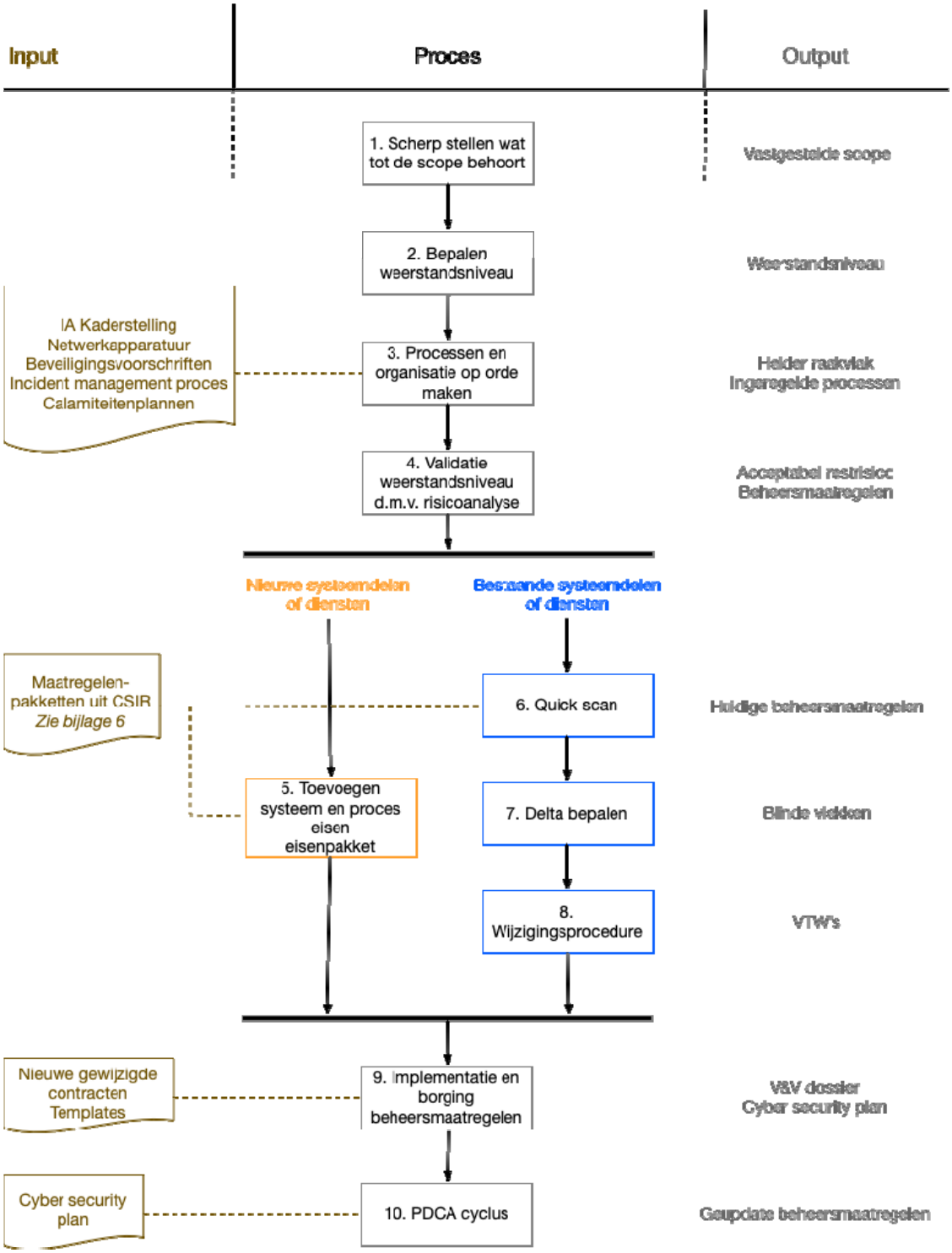
Bijlage 4 geeft een template voor het cybersecurity beveiligingsplan. Deze template wordt door opdrachtnemers gebruikt om plannen op te stellen die beschrijven welke stappen en activiteiten er voor een specifiek project of object worden uitgevoerd.

Omdat de maatregelenpakketten van de CSIR geformuleerd zijn vanuit de RWS context is voor een aantal maatregelen een vertaalslag nodig. Deze vertaalslag heeft geleid tot de generieke maatregelen-set die is opgenomen in bijlage 5. Om de traceerbaarheid met de CSIR te behouden zijn dezelfde ID's gebruikt voor de eisen en is ook de originele eistekst opgenomen.

Daarnaast dient u als DCO de aansluiting met het staande beleid in de eigen organisatie te borgen. Zie hiervoor het stappenplan in de volgende sectie.

3.2 Stappenplan voor toepassen van de CSIR

De stappen die concreet gevolgd moeten worden, zijn weergegeven in onderstaand schema. In de paragrafen die hierop volgen, worden de stappen uit dit schema toegelicht.



Figuur 4 Stappenplan toepassing CSIR binnen DCO

1 Scherpstellen wat tot de scope behoort

De eerste stap is het vaststellen van de scope. Met name in situaties waarin nieuwe systeemdelen en/of iDiensten worden gecombineerd met bestaande systeemdelen en processen is deze stap belangrijk. Wordt er bijvoorbeeld gebruik gemaakt van bestaande netwerkvoorzieningen, blijven delen van bestaande centrales en/of objectbediening, -bewaking en -besturing behouden. Welke opdrachtnemers zijn daarbij betrokken en hoe zit het lopende contract in elkaar?

De antwoorden op deze vragen bepalen wat mee genomen wordt in de rest van de stappen. De output van deze stap is een vastgestelde scope.

2 Bepalen van het weerstandsniveau

De tweede stap is het bepalen van het weerstandsniveau van het onderdeel in de scope. Dit is een strategische keuze van de DCO en wordt gedaan op basis van de impact die risico's kunnen hebben op de bedrijfsvoering. Rijkswaterstaat bepaalt het weerstandsniveau van haar objecten aan de hand van de infraclassificatie. De infraclassificatie is een intern RWS instrument en heeft alleen betrekking op de objecten van RWS. Om die reden moet een DCO zelf een à priori keuze maken voor een weerstandsniveau. Met de risicoanalyse in stap 4 wordt vervolgens deze keuze gevalideerd.

Voor iDiensten en iCentrales is niveau 3 van toepassing tenzij de wegbeheerder bij de aanbesteding anders aangeeft. Als de wegbeheerder dit besluit, kan in het RfP duidelijk hiernaar worden verwezen. Alleen wanneer er sprake is van bediening van zeer kritische objecten (bijvoorbeeld een primaire waterkering zoals de Oosterscheldekering) dan is een verhoging naar weerstandsniveau 4 nodig. Andersom kan indien het belang van het bediende areaal beperkt is, worden volstaan met weerstandsniveau 2.

3 Eigen processen en organisatie gereedmaken

Cybersecurity is maar voor een klein deel techniek en voor een groot deel organisatie en proces. Veel van de beheersmaatregelen die gevraagd worden van opdrachtnemers zijn dan ook procesmatig van aard en gaan over het rapporteren en escaleren van incidenten, het uitvoeren van oefeningen, het beperken van de impact van een incident of het achterhalen van de oorzaak van incidenten.

Vanuit deze maatregelen is interactie vereist tussen opdrachtnemers en de opdrachtgever. Om dit goed te laten verlopen dient opdrachtgever haar zijde van deze raakvlakken in te richten. In bijlage 6 zijn per aandachtsgebied uit de CSIR deze aspecten benoemd. Samengevat is de input de volgende processen, voorschriften en beleidskeuzes:

- IA kaderstelling; DCO beleid voor de inzet van IA.
- Netwerkarchitectuur en aansluitvoorwaarden voor koppelen met het netwerk van de DCO.
- Beveiligingsvoorschriften, zoals wachtwoordrichtlijnen, anti malware voorschriften, huisregels, e.d.
- Incidentmanagement proces en escalatie paden.
- (Regionale) calamiteitenplannen.

In bijlage 6 is terug te vinden met welke maatregelen deze raakvlakken verband houden.

4 Validatie weerstandsniveau d.m.v. risicoanalyse

Met een risicoanalyse worden de risico's in kaart gebracht en krijgen ze een score. De risicoscore wordt opgesplitst in waarschijnlijkheid en impact op belangrijke criteria voor de organisatie.

Om de impact van de cyber-attacks te kunnen inschatten kan gebruik gemaakt worden van het RAMSSHE€P model. (RAMSSHE€P, staat voor Reliablity, Availability, Maintainability, Safety, Security, Health, Environment, Economics en Political) In de "Handreiking prestatie gestuurde risicoanalyses (PRA)" van Rijkswaterstaat is een model uitgewerkt waarbij voor al deze aspecten een mate van ernst van de gevolgen uit te drukken in de categorieën:

1. Verwaarloosbaar;
2. Beperkt;
3. Groot;
4. Ernstig.

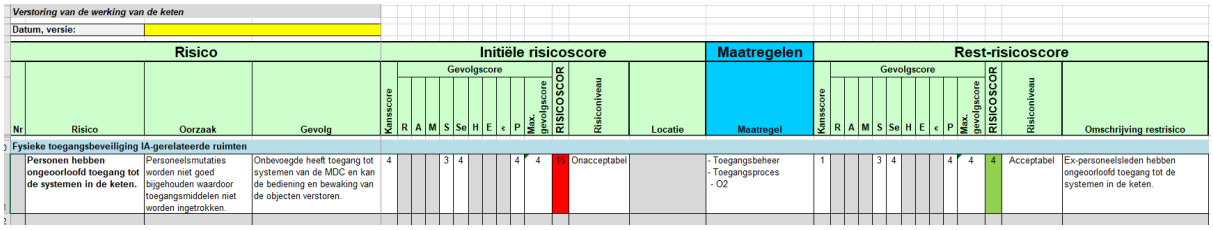
Voor het bepalen van de waarschijnlijkheid van een Cyberattack wordt een inschatting gemaakt op basis van het dreigingsniveau zoals dat jaarlijks door het NCSC (Nationaal CyberSecurity Center) wordt ingeschat in het “Cybersecuritybeeld Nederland” (CSBN).

Door de waarschijnlijkheid en de impact te combineren in een risico-acceptatiematrix wordt zichtbaar hoe noodzakelijk een beheersmaatregel voor het betreffende risico is.

Vervolgens worden per risico de beheersmaatregelen uit de maatregelenpakketten van de CSIR die invloed hebben op de impact of de kans van het betreffende risico geselecteerd. De invloed van de maatregelen wordt gekwantificeerd in de resulterende kans- en impactscore na implementatie van de maatregel. Dit bepaalt de grootte van het restrisico dat overblijft na implementatie van deze maatregelen.

Of een restrisico acceptabel is, hangt van verschillende factoren af. Daarom dient vooraf een kader te worden opgesteld met aanvaarbare risico’s in de vorm van een risico-acceptatiematrix. Hierin wordt vastgesteld welke combinaties van kans en impact op de belangrijke criteria voor de organisatie leiden tot onacceptabele, ongewenste of acceptabele risicoscores. Per domein kunnen er verschillende risico-acceptatieniveaus gelden.

In figuur 5 is hier een voorbeeld van gegeven. Te zien is dat het benoemde risico een niet-acceptabele risico-score heeft (te zien aan de rode kolom). De genomen maatregelen staan weergegeven onder de blauwe cel. Door de genomen maatregelen zal met name de kans van optreden van dit risico afnemen, waardoor de risicoscore lager uitvalt. Dit is te zien aan de groene cel. De risicoscore die overblijft na het nemen van bepaalde maatregelen is de rest-risicobepaling.



Verstoring van de werking van de keten																												
Datum, versie:																												
Risico				**Initiële risicoscore**													**Maatregelen**	**Rest-risicoscore**											
					Gevolgscore														Gevolgscore										
Nr	Risico	Oorzaak	Gevolg	Kansscore	R	A	M	S	Se	H	E	€	P	Max. gevolgscore	RISICOSCOR	Risiconiveau	Locatie	Maatregel	Kansscore	R	A	M	S	Se	H	E	€	P	Max. gevolgscore	RISICOSCOR	Risiconiveau	Omschrijving restrisico
Fysieke toegangsbeveiliging IA-gerelateerde ruimten																															
	Personen hebben ongeoorloofd toegang tot de systemen in de keten.	Personeelsmutaties worden niet goed bijgehouden waardoor toegangsmiddelen niet worden ingetrokken.	Onbevoegde heeft toegang tot systemen van de MDC en kan de bediening en bewaking van de objecten verstoren.	4				3	4				4	4	16	Onacceptabel		- Toegangsbeheer - Toegangsproces - O2	1				3	4				4	4	4	Acceptabel	Ex-personeelsleden hebben ongeoorloofd toegang tot de systemen in de keten.

Figuur 5 Voorbeeld van de risico-acceptatiematrix

Door op deze manier de rest-risicobepaling te doen met de verantwoordelijke proces- en systeemeigenaren, wordt bepaald of het a-priori weerstandsniveau en bijbehorende maatregelen de risico’s tot een aanvaardbaar rest-risico hebben teruggebracht.

In samenhang met de QuickScan is daarmee tegelijk duidelijk welke maatregelen geïmplementeerd moeten worden op de bestaande systemen om te komen tot een acceptabel risicoprofiel.

5 Toevoegen systeem- en proceseisen

Voor nieuwe te realiseren systeemdelen of af te nemen diensten, dienen in de programma’s van eisen de informatiebeveiligingseisen meegegeven te worden bij de aanbesteding. Deze eisen zijn in bijlage 6 opgenomen. In bijlage 6 wordt verwezen naar de Verwerkersovereenkomst die als bijlage 7 is opgenomen.

Als input voor bijlage 6 zijn de eisen van RWS gebruikt, die zijn opgenomen in bijlage 1 en 2. De eisen bestaan uit een aantal systeem- en proceseisen die vervolgens doorverwijzen naar concrete maatregelen in de CSIR maatregelpakketten en de onderliggende richtlijnen. Bijlage 1 is specifiek ontwikkeld voor natte projecten, maar is eveneens toepasbaar op droge projecten en iDiensten.

De volgende stap na deze stap 5 is stap 9. Stap 6, 7 en 8 zijn voor bestaande systeemdelen.

6 Quick scan

Voor de bestaande systeemdelen die behouden blijven wordt een quick scan uitgevoerd. Deze scan fungeert als nulmeting. Dit geeft inzicht in welke beheersmaatregelen al genomen zijn, welke informatiebeveiligings-processen geïmplementeerd zijn en op welke gebieden juist nog blinde vlekken zijn. Hiermee wordt duidelijk waar aanvullende maatregelen nodig zijn in de bestaande omgeving.

De quick scan wordt uitgevoerd op basis van de maatregelpakketten uit de CSIR. De maatregelenpakketten zijn opgenomen in bijlage 1 en 2 en bestaan uit een aantal systeem- en proceseisen en gelden als input voor deze stap. Tijdens de quick scan wordt per maatregel uit de CSIR voor het geselecteerde weerstandsniveau tijdens een interview met experts vastgesteld of de maatregel is ingevuld. Omdat de maatregelenpakketten van de CSIR

geformuleerd zijn vanuit de RWS context, is het te verwachten dat in de bestaande omgeving van een DCO maatregelen niet één-op-één vergelijkbaar zijn ingevuld. Enige vrijheid van interpretatie van de maatregel is daarom nodig.

Om deze interpretatie eenvoudiger te maken zijn de RWS maatregelen vertaalt naar een generieke maatregelenset die is opgenomen in bijlage 5. Om de traceerbaarheid met de CSIR te behouden zijn dezelfde ID's gebruikt voor de eisen en is ook de originele eistekst opgenomen.

7 Delta bepalen

Uit de resultaten van de quick scan blijkt welke maatregelen in de bestaande delen die behouden blijven onvoldoende zijn ingevuld. Dit is de delta van de huidige situatie ten opzichte van de gewenste situatie.

Deze delta zal opgelost moeten worden om tot een beheerste eindsituatie te komen. In overleg met de proces-, systeemeigenaren en de CISO dient vastgesteld te worden op welke wijze en binnen welke termijnen deze achterstand ingelopen gaat worden.

8 Wijzigingsprocedure

Het resultaat van de delta bepaling leidt tot één of meerdere wijzigingsverzoeken richting de beheerorganisatie(s) van de systeemdelen waarom het gaat. Deze wijzigingen zullen het bestaande reguliere wijzigingsproces doorlopen zoals dat gehanteerd wordt bij de DCO en zoals dat is overeengekomen met bestaande opdrachtnemers.

De beheersmaatregelen uit de CSIR omschrijven hierbij de eisen op het gebied van cybersecurity die via deze wijzigingen worden toegevoegd aan het bestaande systeem. Deze zijn opgenomen in bijlage 2.

9 Implementatie en borging van de beheersmaatregelen

Zowel in de nieuwe delen en diensten als in de behouden bestaande systeemdelen en dienstverlening worden de maatregelen, zoals in de voorgaande stappen bepaald, geïmplementeerd. Dit zijn de contracten met de wijzigingen. Onlosmakelijk hiermee verbonden is de verificatie dat genoemde maatregelen zijn geïmplementeerd en validatie dat de risico's voldoende zijn beheerst.

Wanneer gestandaardiseerde producten en/of diensten worden afgenomen zal de leverancier eenvoudig kunnen aantonen via keuringen of certificeringen dat het ontwerp een groot deel van de maatregelen afdekt. Voor de project- of klantspecifieke invulling zal de leverancier specifieke verificaties moeten uitvoeren. In bijlage 4 is de template opgenomen dat RWS hiervoor ter beschikking stelt aan haar opdrachtnemers.

Vanuit de BIO is aantoonbaarheid zeer belangrijk. De verantwoordelijkheid voor het integraal toetsen of aan de eisen is voldaan ligt vanuit de BIO altijd bij opdrachtgever.

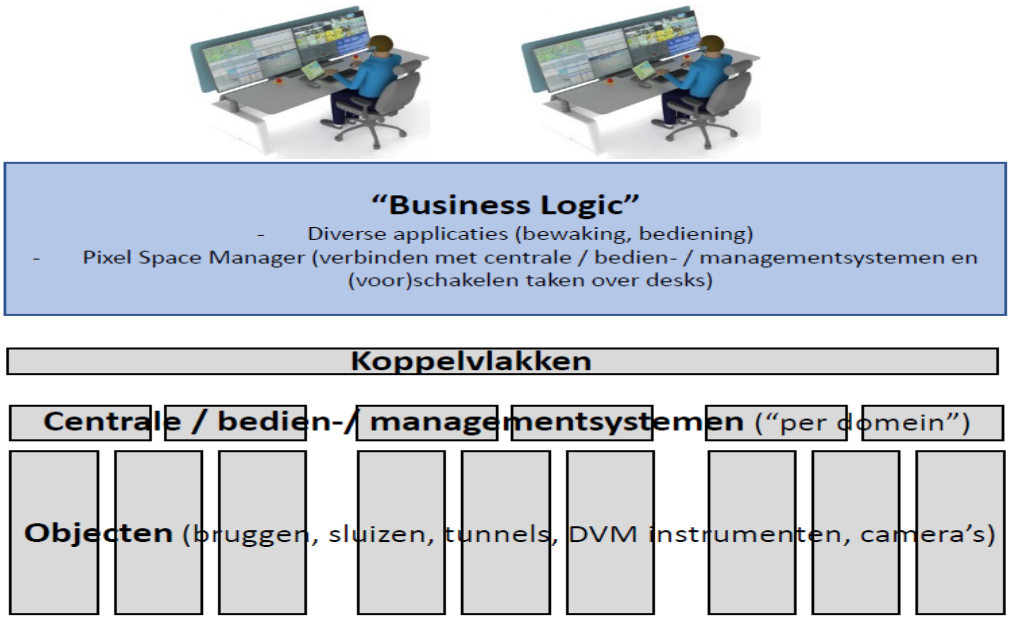
10 PDCA-cyclus

Het is zaak dat de maatregelen vervolgens periodiek worden geëvalueerd en eventueel worden bijgesteld. Om dit planmatig uit te voeren is het raadzaam om een cybersecurity plan op te stellen. Dit plan is dan ook de input voor deze processtap.

4 Casebeschrijving MultiDomein Centrale Hoofddorp

In dit hoofdstuk is een casebeschrijving gegeven van de implementatie van cybersecurity bij de MultiDomein Centrale (MDC) te Hoofddorp waarbij gebruik gemaakt is van de hiervoor beschreven aanpak. Deze case is als voorbeeld toegevoegd omdat de aanpak heeft geleid tot een succesvolle implementatie.

De provincie Noord-Holland heeft kortgeleden het realisatieproject MultiDomein Centrale (MDC) Hoofddorp afgerond. Het betreft het slim 'combineren en integreren' van 3 bestaande PNH bediencentrales door middel van een intelligente (ICT-)toplaag. Op deze wijze worden de 3 PNH bediencentrales met elkaar verbonden. De daadwerkelijke toplaag of iCentrale-intelligentie bestaat uit een relatief dunne integrerende systeemlaag over de bestaande systemen en applicaties heen. Deze laag zorgt dat de 3 PNH bediencentrales integraal samenwerken.



Figuur 6 Bestaande bediencentrales en de (ICT-) toplaag die momenteel wordt toegevoegd

De MDC Hoofddorp vormt een klein onderdeel van het automatiseringslandschap dat ingezet wordt om verkeersmanagement, brugbediening en tunnelbediening te organiseren. Doordat het de andere systeemdelen met elkaar verbindt, is het vanuit cybersecurity oogpunt echter wel een belangrijk systeemonderdeel. Bovendien is er een groeiend besef dat een cyberincident grote ongewenste gevolgen kan hebben in de totale keten van MDC Hoofddorp en de daaronder liggende applicaties en systemen, gezien het belang van de onderliggende fysieke systeemdelen (bruggen, sluizen, tunnels en verkeer). Daarom is het noodzaak om de informatie-beveiliging van de MDC Hoofddorp goed te borgen. Dit maakt onderdeel uit van een goede borging van de informatiebeveiliging van de totale keten.

4.1 Hoe zijn de stappen specifiek ingevuld?

Scherpstellen wat tot de scope behoort

Als eerste is formeel vastgesteld welke delen van de organisatie, processen en/of systemen tot de scope behoren. Voor de MDC is de scope vastgesteld op de ICT toplaag en de Centrale bedien- en management-systemen van de domeinen verkeersmanagement, tunnelbediening en brug- en sluisbediening.

De onderliggende besturing van de objecten is buiten beschouwing gelaten.

Bepaling weerstandsniveau

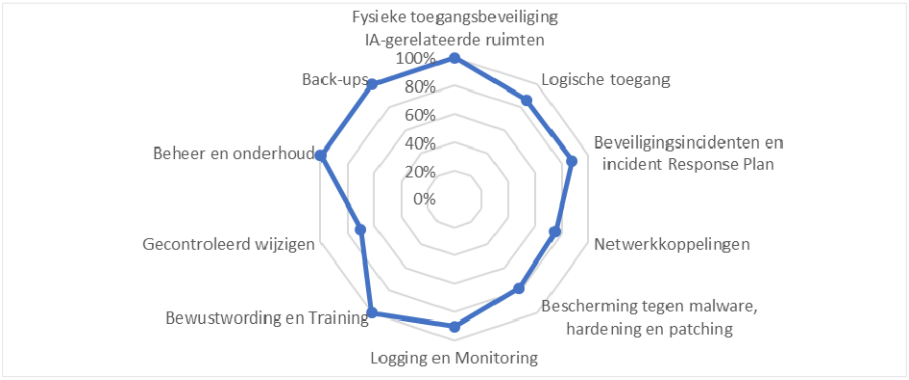
De volgende stap is het bepalen van het weerstandsniveau. Zoals eerder is aangegeven maakt de methode van Rijkswaterstaat gebruik van 4 weerstandsniveaus.

Figuur 7 Verkeerscentrale Provincie Noord-Holland, Hoofddorp

Om het à priori weerstandsniveau voor de MDC Hoofddorp te bepalen, is de vergelijking gemaakt naar objecten binnen de RWS-context met vergelijkbare functie en impact. De verkeerscentrales en bediencentrales van RWS zijn over het algemeen ingeschaald op weerstandsniveau 3. Om deze reden is voor de MDC Hoofddorp ook gekozen voor niveau 3.

Quickscan

Na het bepalen van het weerstandsniveau is de quickscan uitgevoerd. Voor de ICT-toplaag en per bestaand PNH domein is aangegeven aan hoeveel procent van het aantal eisen uit de CSIR wordt voldaan (zie figuur 8 als voorbeeld). Opgemerkt moet worden dat een laag percentage niet per definitie betekent dat de risico's onvoldoende beheerst zijn. Bij een hoog percentage is de aanname dat het risico voldoende gemitigeerd is wel gerechtvaardigd, bij een lager niveau kan het betekenen dat het risico onvoldoende beheerst wordt. Het kan echter ook zo zijn dat op een andere wijze, dan met de maatregelen als beschreven in de CSIR, het risico wel voldoende wordt beheerst.



Figuur 8 Voorbeeld resultaat quickscan van 1 domein.

In deze fase is er vooral energie gestoken in het bepalen of er wordt voldaan aan een eis uit de CSIR. Hoe deze wordt aangetoond en waar deze bewijslast staat, is nog niet van belang omdat het hier puur om een referentie-meting gaat. Uiteindelijk is het wel degelijk van belang dat het voldoen aan de Cybersecurity-eisen aantoonbaar is. Om deze reden is, voor het beoordelen van de resultaten van de quickscan, de volgende indeling gemaakt:

Score	Oordeel
80-100%	Voldoende
< 80%	Expert judgement nodig om mate van beheersing vast te stellen.

Validatie weerstandsniveau d.m.v. risicoanalyse

Na een eerste inventarisatie door middel van de quickscan, is gevalideerd of het gekozen weerstandsniveau wel de juiste noodzaak en diepgang van maatregelen biedt. Uitgaande van de toprisico's, met input van de beheerders en de gebruikers vanuit de betrokken domeinen, is inzichtelijk gemaakt welke delen van de keten/processen door een cyber-attack geraakt kunnen worden en wat de gevolgen hiervan zijn. Hierbij zijn de risicoscore opgesplitst in impact en waarschijnlijkheid.

Om de impact van de cyber-attacks te kunnen inschatten is een risicoanalyse uitgevoerd. De Provincie Noord-Holland gebruikt voor risicoanalyse in het kader van assetmanagement haar eigen risicoscoringsmethodiek, de zogenaamde bedrijfswaardenmatrix. Net zoals de Prestatie gestuurde risicoanalyses (PRA)" van Rijkswaterstaat is dit een model waarbij de ernst van de gevolgen worden uitgedrukt in impact op de bedrijfsdoelstellingen.

Door de waarschijnlijkheid en de impact te combineren in een risico-acceptatiematrix wordt zichtbaar hoe noodzakelijk een beheersmaatregel voor het betreffende risico is. Per domein gelden er verschillende risico-acceptatieniveaus. Tevens is het werkgebied van de geïntegreerde centrale hierin een bepalende factor.

Ernst		Doorstroming									Leefbaarheid		Veiligheid	Imago	Kosten		Kans optreden ongewenste gebeurtenis					
		Ongeplande Niet-Beschikbaarheid									Beeldkwaliteit			Publiciteit	Kosten incident		minder vaak dan 1 x per 30 jaar	1 x per 30 jaar of vaker	1 x per 10 jaar of vaker	1 x per 5 jaar of vaker	1 x per jaar of vaker	1 x per week of vaker
		Stroomwegen / OV	Overige wegen / fietspaden	Basisnet beroepsvaart en staandemast routes	Overige vaarwegen	DVM					Stroomwegen / OV / Fietspaden	Overige wegen										
						VRI			DRIP's	VC												
						Prio 1	Prio 2	Prio 3	Totale areaal	Totale keten												
6	Catastrofaal	> 1 week niet beschikbaar								> 2 dagen niet beschikbaar			Het falen leidt direct of indirect tot ongelukken met: - zeker fataal letsel bij één of meer personen	Internationaal negatief in de pers	> €10.000.000	6						
5	Ernstig	1 dag tot een week niet beschikbaar	> 1 week niet beschikbaar	> 1 week niet beschikbaar		> 1 week niet beschikbaar			> 10 dagen niet beschikbaar	1 tot 2 dagen niet beschikbaar			Het falen leidt direct of indirect tot ongelukken met: - mogelijk fataal letsel bij één of meer personen - zeker blijvend letsel bij één of meer personen	Landelijk negatief in de pers	> €1.000.000	5						
4	Behoorlijk	4 uur tot een dag niet beschikbaar	1 dag tot een week niet beschikbaar	1 dag tot een week niet beschikbaar	> 1 week niet beschikbaar	2 dagen tot 1 week niet beschikbaar	> 1 week niet beschikbaar		5 tot 10 dagen niet beschikbaar	12 tot 24 uur niet beschikbaar	Beeldkwaliteit van een object onder niveau C		Het falen leidt direct of indirect tot ongelukken met: - onwaarschijnlijk fataal letsel bij één of meer personen - mogelijk blijvend letsel bij één of meer personen	Provincial negatief in de pers	> €100.000	4						
3	Matig	1 uur tot 4 uur niet beschikbaar	4 uur tot een dag niet beschikbaar	4 uur tot een dag niet beschikbaar	1 dag tot een week niet beschikbaar	1 tot 2 dagen niet beschikbaar	2 dagen tot 1 week niet beschikbaar	> 1 week niet beschikbaar	1 tot 5 dagen niet beschikbaar	4 tot 12 uur niet beschikbaar	Beeldkwaliteit van een object onder niveau B	Beeldkwaliteit van een object onder niveau C	Het falen leidt direct of indirect tot ongelukken met niet-blijvend letsel met medische assistentie/ ziekenhuis opname bij één of meer personen	Regionaal negatief in de pers	> €10.000	3						
2	Klein	< 1 uur niet beschikbaar	1 uur tot 4 uur niet beschikbaar	1 uur tot 4 uur niet beschikbaar	4 uur tot een dag niet beschikbaar	1 uur tot 1 dag niet beschikbaar	1 tot 2 dagen niet beschikbaar	2 dagen tot 1 week niet beschikbaar	1 uur tot 1 dag niet beschikbaar	1 tot 4 uur niet beschikbaar			Het falen leidt direct of indirect tot ongelukken met niet-blijvend letsel zonder verzuim bij meerdere personen	Lokaal negatief in de pers	> €1.000	2						
1	Verwaarloosbaar		< 1 uur niet beschikbaar	< 1 uur niet beschikbaar	1 uur tot 4 uur niet beschikbaar	< 1 uur niet beschikbaar	1 uur tot 1 dag niet beschikbaar	1 tot 2 dagen niet beschikbaar	< 1 uur niet beschikbaar	< 1 uur niet beschikbaar			Het falen leidt direct of indirect tot ongelukken met niet-blijvend letsel zonder verzuim bij één persoon	Interne negatieve melding	< €1.000	1						

Figuur 9 Voorbeeld Bedrijfswaardenmatrix

Na het vaststellen van de verschillend risico-acceptatieniveaus is het restrisico bepaald. Dit is bepaald door het effect van de maatregelpakketten, behorend bij het gekozen weerstandsniveau, te vertalen naar een verlaging van de kansen en/of impact. In afbeelding 8 is dit weergegeven. Te zien is dat het benoemde risico een niet-acceptabele risicoscore heeft (te zien aan de rode kolom). De genomen maatregelen staan weergegeven in onder de blauwe cel. Door de genomen maatregelen zal het risico afnemen, waardoor ook de risicoscore lager uitvalt. De mate waarin een maatregel effect heeft op de kans of de impact blijft een vorm van expert-judgement. Het effect van de aangepast kans-waarde is te zien aan de groene cel. De risicoscore die overblijft na het nemen van bepaalde maatregelen is de rest-risicobepaling.

Risico				Initiële risicoscore									Maatregelen	Rest-risicoscore									
					Gevolgscore										Gevolgscore								
Nr	Risico	Oorzaak	Gevolg	Kanscore	Doorstroming	Leefbaarheid	Veiligheid	Imago	€	Max. gevolgscore	RISICOSCORE	Risiconiveau	Maatregel	Kanscore	Doorstroming	Leefbaarheid	Veiligheid	Imago	€	Max. gevolgscore	RISICOSCORE	Risiconiveau	Omschrijving restrisico
	Toegang tot het systeem voor bedienaars is geblokkeerd	Personeelsmutaties worden niet goed bijgehouden waardoor toegangsmiddelen niet worden ingetrokken.	Onbevoegde heeft toegang tot systemen van de MDC en kan de bediening en bewaking van de objecten verstoren.	4	4			3	3	4	16	Onacceptabel	- Toegangsbeheer - Toegangsproces - O2	2	2			1	1	2	4	Acceptabel	Ex-personeelsleden hebben ongeoorloofd toegang tot de systemen in de keten.

Figuur 10 Voorbeeld risico-acceptatiematrix van de Provincie Noord-Holland

Op basis van deze rest-risicobepaling hebben de verantwoordelijke proces- en systeem eigenaren bepaald of het a-priori weerstandsniveau en bijbehorende maatregelen de risico's tot een aanvaardbaar rest-risico hebben teruggebracht. Op deze wijze is traceerbaar en aantoonbaar gemaakt dat het gekozen weerstandsniveau (3) in lijn is met het staande beleid van de Provincie Noord-Holland.

Implementatie & borging van beheersmaatregelen

Na het valideren van het gekozen weerstandsniveau is daarmee ook bekend welk maatregelenpakket geïmplementeerd moeten worden, aangezien elk niveau zijn specifieke maatregelenpakket heeft.

Het maatregelenpakket is gekozen op basis van de RWS-maatregelen, maar deze zijn niet 1-op-1 toepasbaar voor de provincie. Daarom zijn de maatregelen ontdaan van de RWS-specifieke maatregelen. Dit heeft geleid tot een vertaling van de maatregelen uit de RWS-CSIR naar generiek toepasbare systeem- en proceseisen (zie bijlage 6). Bovendien zijn deze eisen direct gerelateerd aan de BIO, zodat ook inzichtelijk wordt in hoeverre de beheersdoelen van de BIO behaald zijn.

Het is voor de borging en het beheer van belang dat de genomen maatregelen worden afgestemd en ingepast in de huidige processen en methodieken. Deze processen en methodieken zijn immers al bekend bij de medewerkers.

Na het implementeren van de beheersmaatregelen is het van belang dat de maatregelen periodiek worden geëvalueerd zodat kwaliteitsborging en -verbetering op kan treden. Met deze laatste stap wordt is Plan-Do-Check-Act-cirkel (PDCA) gesloten. Vastlegging van de bevindingen vormen de basis om aan te kunnen tonen dat aan de BIO invulling is gegeven.

4.2 Lessons learned

Bij de toepassing van deze aanpak bij de Provincie Noord-Holland, zijn de volgende 'lessons learned':

- Door het verder integreren en koppelen van eerder onafhankelijk systemen, ontstaan nieuwe risico's en kwetsbaarheden welke aanvullend moeten beoordeeld. Daarbij is de methode van waarde gebleken om snel inzichtelijk te krijgen wat deze extra risico's zijn, en welke aanvullende maatregelen genomen moeten worden op het reeds bestaande beveiligingsniveau.
- De stapsgewijze aanpak van Rijkswaterstaat structureerde het proces. De CSIR wordt vaker gebruik in de sector en is daarom herkenbaar, wat het een efficiënt proces maakt.
  De verificatie of wordt voldaan aan een beheersmaatregel kan subjectief zijn. Stel daarom eerst vast hoe gaat worden aangetoond dat wordt voldaan. Vervolgens kan door middel van bewijslast zoals afgesproken de verificatie objectief worden gedaan.

Literatuurlijst

(2019). Cybersecuritybeeld Nederland. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

(12 juni 2019). Kamerbrief Beleidsreactie CSBN2019 en voortgangsrapportage NCSA. Ministerie van Justitie en veiligheid.

Begrippenlijst

Cybersecurity

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

Informatievoorziening (IV)

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

Industriële Automatisering (IA)

Industriële Automatisering omvat de ICS/SCADA systemen en de ICT gerelateerde systemen en onderdelen (hardware en software), waarbij functioneel interactie plaats vindt met de fysieke omgeving of gebruikers (bijvoorbeeld een brug, onderstation, DRIP, etc.). Dit omvat mede het verkrijgen van informatie over de fysieke omgeving (inwinnen) en het beïnvloeden van de fysieke omgeving (bedienen en besturen). Wij hanteren hier de terminologie IA en KA (Kantoor Automatisering). Een andere benaming die veel gebruikt wordt is IT (Informatie technologie) en OT (operationele technologie)

Informatie- en Communicatietechnologie (ICT)

Informatie- en Communicatietechnologie omvat een samenhangend geheel van informatiesystemen, hardware en software, operating systemen van servers, de onderliggende technische datanetwerkinfrastructuur met data-netwerken en bijbehorende datanetwerkcomponenten, dataopslag in rekencentrum, computer- en technische ruimten met als doel het mogelijk maken of ondersteunen van de processen.

Industrial Control Systems (ICS)

Industrial Control Systems zijn systemen die toegerust zijn voor de bediening en besturing van de RWS Infra-structuur waarbij ook gebruik wordt gemaakt van SCADA systemen.

Supervisory Control And Data Acquisition (SCADA)

SCADA systemen verzamelen, verwerken en visualiseren meet- en regelsignalen.

RWS Infrastructuur

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

Deel B

Cybersecurity Implementatierichtlijn Objecten – RWS

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

Inhoudsopgave

1 Inleiding

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

1.1 Baseline Informatiebeveiliging RWS

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

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

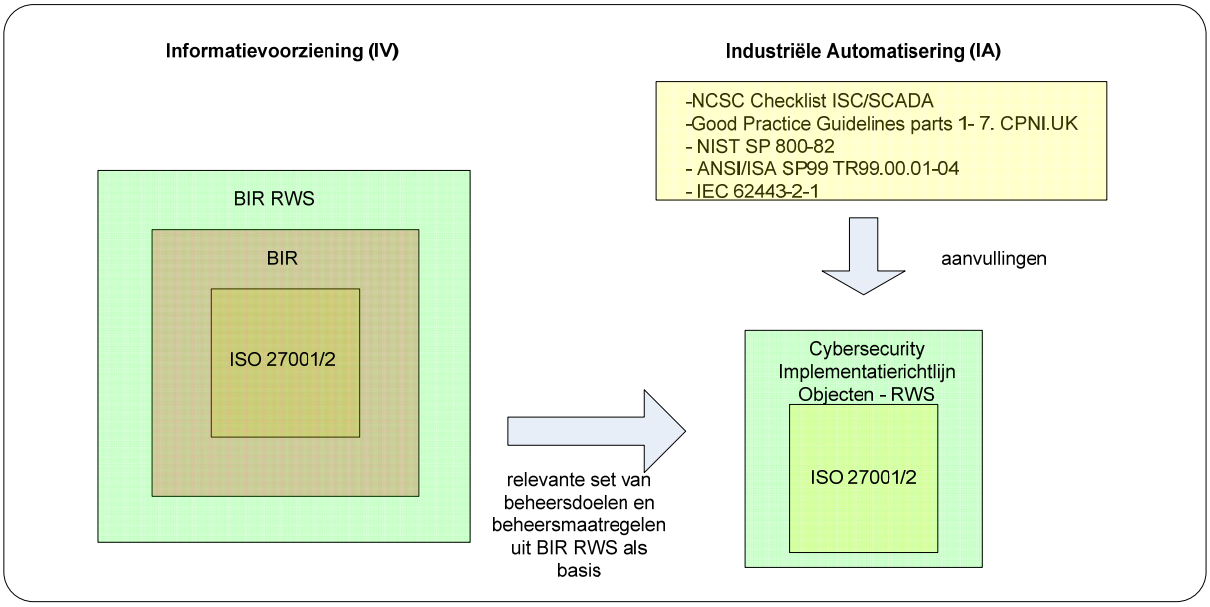
1.2 Cybersecurity Implementatierichtlijn Objecten - RWS

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

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

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

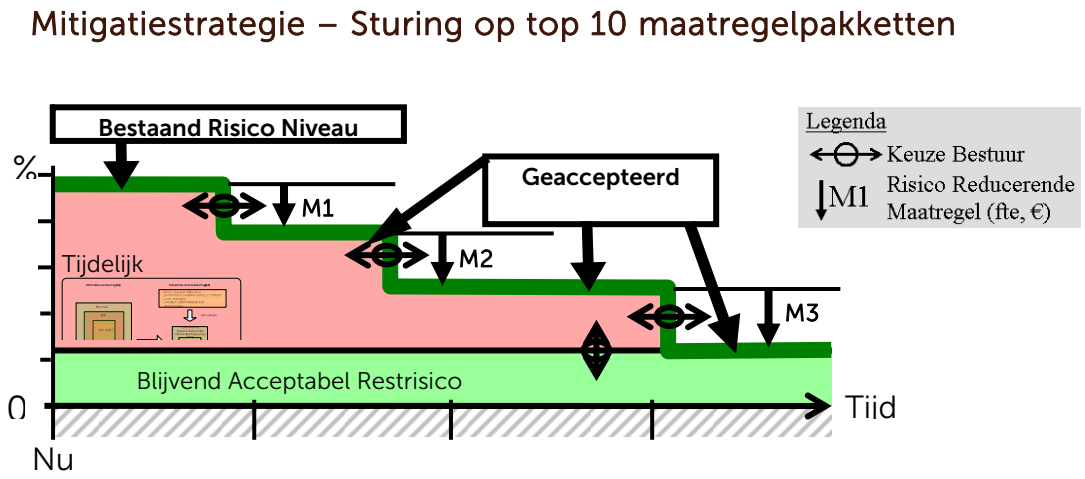
Afhankelijk van het domein, het karakter van de samenwerking, de uitbesteding van taken en de operationele behoefte neemt RWS binnen de kaders van het beveiligingsbeleid van IenM de ruimte om afgeleide implementatierichtlijnen uit de BIR RWS te ontwikkelen en van toepassing te verklaren zoals de Cybersecurity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



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

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

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



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, op te vragen bij PRIA of CIV-IRN/Security Center). 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 weerstands-niveau.

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

Voorbeeld

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

1.4 Structuur

In het contract zijn de relevante beheersdoelen (lees Cybersecurity beveiligingseisen) en beheersmaatregelen beschreven die afgeleid zijn uit de BIR (RWS). Naast de Cybersecurity beveiligingseisen uit de BIR RWS zijn tevens de relevante Cybersecurity beveiligingseisen en beheersmaatregelen uit de NCSC Checklist beveiliging ICS/SCADA systemen opgenomen in het contract. Indien noodzakelijk worden vanuit de proces- en systeem-eisen verwezen naar de maatregelpakketten waar een verdieping plaatsvindt in de maatregelenset en dit is weer afhankelijk van het risico en het cybersecurity weerstandsniveau dat gehaald moet worden.

Hoofdstuk 2 beschrijft de maatregelpakketten die een verdieping of aanvulling vormen op de Cybersecurity beveiligingseisen. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS hanteert. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS. Afhankelijk van de infraclassificatie en de daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maat-regelpakketten 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 hoofdstuk 3 is de wachtwoord richtlijn opgenomen en in hoofdstuk 4 de Factsheet Wachtwoorden.

2 Specifieke maatregelpakketten

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

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

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

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

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

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

2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten

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

N.B.:

1. Naast bovengenoemde weerstandsniveaus 1 t/m 4 zijn door de DG en politieke top specifieke maat-regelenpakketten 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.

2.2 Maatregelen Logische toegang

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

Mens	LTM1	Voor bewustwording, gedragsregels en training van, bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training"
Procedures & Organisatie	LTPO1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.
	LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend op basis van het 'need to have' principe plaatsvindt; • de toewijzing en het gebruik van privileges van administrators en systeem-beheerders 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	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die RWS hiervoor beschikbaar stelt.
	LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – minimaal een user-id en wachtwoord combi-natie 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 wijzigings-verzoek of storingsmelding. De toegang wordt bewaakt en teruggezet bij af-melding van de call.
Techniek	LTT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.
	LTT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.
	LTT3	Voor bedienaars en beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

2.3 Maatregelen Beveiligingsincidenten en incident Response Plan

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

Mens	BIRPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen security incidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen moet worden geëist dat zij alle security incidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.
	BIRPO2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.
	BIRPO3	Er is bestaat een geborgde procedure voor de reactie op en eventuele escalatie van security incidenten. De security incidenten worden vastgelegd, gerappor-teerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aan-spreekbaar zijn inzake storingen, security incidenten 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	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incidentmanager van RWS-CIV ingeschakeld.
	BIRPO6	Er dient een geborgde procedure te bestaan voor incidentrespons ingeval van incidenten en calamiteiten.
	BIRPO7	Jaarlijks dienen de incident responseplannen beproefd te worden aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van incidentresponse is het testen van de noodbediening.

Techniek	BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

2.4 Maatregelen Netwerkkoppelingen

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

Mens	NKM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van 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 netwerk-diensten 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 aansluit-voorwaarden 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 Object-verantwoordelijke/-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 en ziet erop toe dat het lokale objectdata-netwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie ‘Maatregelen bescherming tegen malware, hardening en patching’).
	NKPO6	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.
	NKPO7	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door middel van een Configuration Management Database (CMDB).
	NKPO8	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en op-volging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit RWS-CIV.
Techniek	NKT1	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige

		communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
	NKT2	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.

2.5 Maatregelen bescherming tegen malware, hardening en patching

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

Mens	MHPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van 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	De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.
	MHPPO4	De Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
	MHPPO5	Opdrachtnemer dient over een geborgde procedure te beschikken voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden.
	MHPPO6	Bij patches en anti-virusupdates, die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.
	MHPPO7	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging schriftelijk te worden vastgelegd voorzien van een risicoafweging.
	MHPPO8	Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
	MHPPO9	Voor zover technisch te scannen dienen zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te worden gescand.

	MHPPO10	Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op malware gecontroleerd worden voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
Techniek	MHPT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.
	MHPT2	Antimalware voorzieningen moeten in afstemming met RWS-CIV ingezet worden.

2.6 Maatregelen Logging en Monitoring

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

Mens	LMM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van 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 drie maanden bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
	LMPO3	Voor de levering van logbestanden aan derden dient de RWS Objectverant-woordelijke/-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 gegevens-overdrachten tussen het ICS/SCADA en gekoppelde ICT-componenten in kaart

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

2.7 Maatregelen Bewustwording en Training

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

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

		- niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
	BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.
	BTME7	Opdrachtnemer, Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
	BTME8	Bedienaars, beheerders en overig ondersteunend 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	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
	BTME10	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.
	BTME11	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.
	BTME12	Voor Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
	BTME13	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
	BTME14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.
	BTME15	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te 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 Opdrachtnemer dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
	BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
	BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontrolepro-grammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.

	BTME19	Gegevensdragers worden altijd vooraf op malware gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
	BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME22	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur - zo mogelijk - wordt gelocked.
Manager	BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt door Opdrachtnemer 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 Opdrachtnemer/objectverantwoordelijke/-beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.
	BTMA4	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.

2.8 Maatregelen gecontroleerd wijzigen

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

Mens	GWM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van 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. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.
	GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.
	GWPO4	Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen dient altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten voordat uitvoering van werkzaamheden plaatsvindt zijn goedgekeurd door de Objectverantwoordelijke/ -beheerder.
	GWPO5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/ configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.
	GWPO6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten indien mogelijk vooraf aan de implementatie in productie te worden getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit of beveiliging van de organisatie. Indien haalbaar moet voor ICS/SCADA en overige ondersteunende ICT-systemen controle worden uitgevoerd voor de authenticiteit/integriteit van de software voorafgaande aan de implementatie op operationele systemen.
	GWPO7	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.

2.9 Maatregelen beheer en onderhoud

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

Mens	BOM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van 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 over-eengekomen 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 ICT en IA 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 en ziet erop toe dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.
	BOPO8	Opdrachtnemer dient jaarlijks de opzet, bestaan en werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever.
Techniek	BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.
	BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV.

Good Practice - Maatregelen personele toegang

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

- een persoonlijke geheimhoudingsverklaring ondertekent en overhandigt aan de Opdrachtgever;
- zich daarbij legitimeert en een goed gelijkende pasfoto overhandigt aan de Opdrachtgever;
- een Verklaring Omtrent Gedrag (VOG) bezit en een kopie daarvan aan de Opdrachtgever overlegt welke is gerelateerd aan de beoogde Werkzaamheden.

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

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

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

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

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

2.10 Maatregelen Back-ups

Niveau	Mens	Procedures & Organisatie	Techniek
4	BUM 1	BUPO 1 t/m 5	BUT 1
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 vooraf en na iedere (functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd, met deze back-up moet men in staat zijn een volledige roll-back naar de werkende situatie terug te kunnen gaan; • Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevind; • Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de

		hoofdlocatie en zijn alleen toegankelijk voor bevoegden; • Back-ups worden bewaard tot het moment van uitdienstname van betreffend systeem; • Ingeval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.
	BUPO3	Er bestaan gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.
	BUPO4	Herstelprocedures moeten jaarlijks worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd. Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is. Herstelprocedures zijn onderdeel van de disaster recovery planning.
	BUPO5	Door 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.

3 Wachtwoorden 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/wachtwoord-combinaties 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

4 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. Hoofdstuk 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 hoofdstuk 3 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

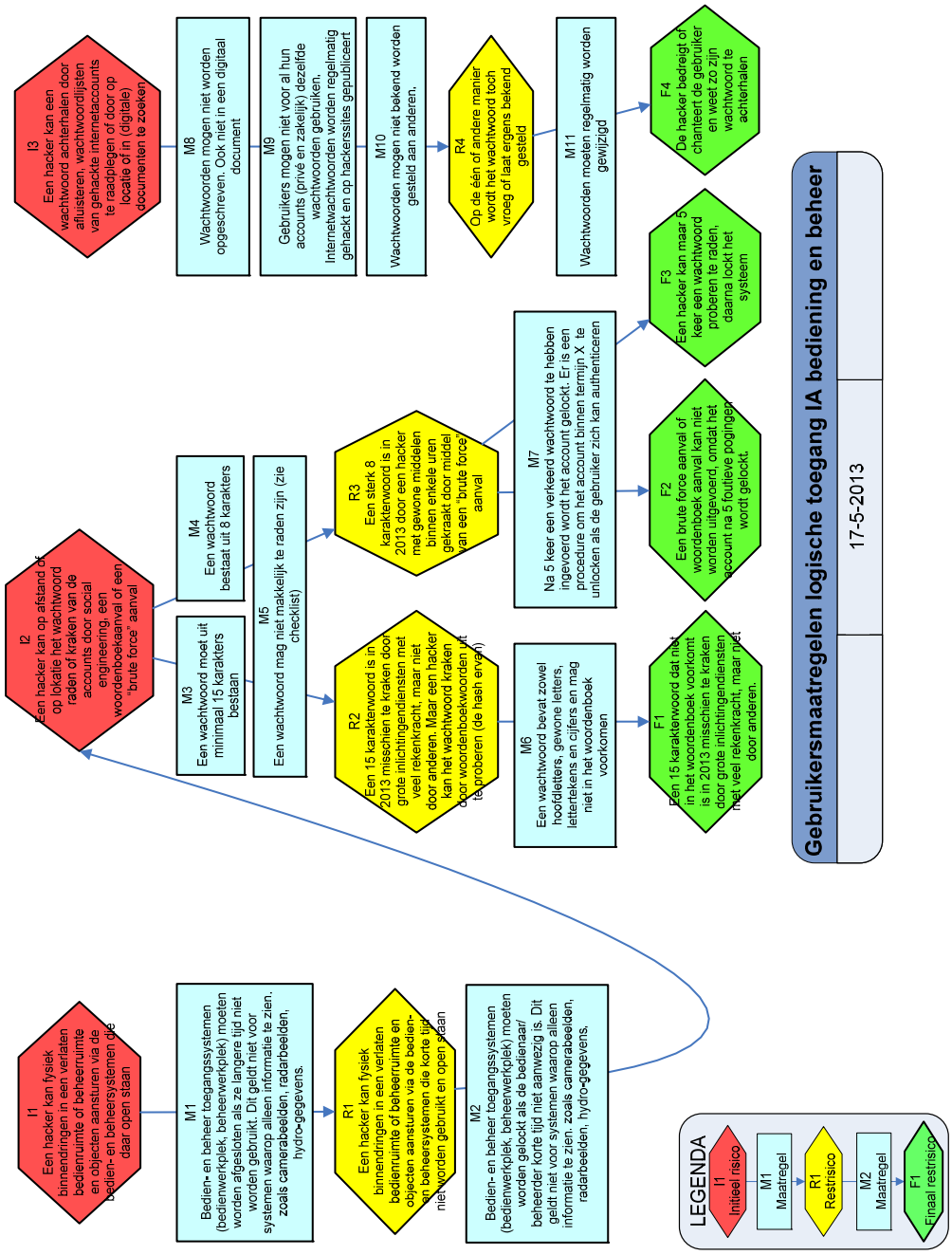
1. Als bedienaars of beheerders een bedien- of beheerruimte langere tijd geheel verlaten, dienen zij het bedien- of beheerstation af te sluiten.
2. Als bedienaars of beheerders een bedien- of beheerruimte korte tijd geheel verlaten, dienen zijn het bedien- of beheerstation te locken.

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.

Gebruikersmaatregelen

Risicoreductieoverzicht logische toegang IA bediening en beheer vanuit gebruikersperspectief



Bijlagen

Bijlage 1 Standaard Systeemeisen Cybersecurity – Natte projecten

Uitgegeven door	RWS/CIV/SC
Vertrouwelijkheidsniveau	RWS Ongeclassificeerd
Datum	25 april 2016
Versie	1.1

Systeem topeis: Cybersecurity
Het Systeem dient voor cybersecurity zodanig te worden ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.

Cybersecurity weerstandsniveau
Het Systeem dient daar waar in deze overeenkomst direct of indirect verwezen wordt naar de specifieke implementatie richtlijnen uit de "Cybersecurity Implementatierichtlijn Objecten-RWS" te voldoen aan het cybersecurity weerstandsniveau [xxx].

Gelaagde beveiliging
Het Systeem dient de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging uitgevoerd te hebben.

Fysieke beveiliging
Het Systeem dient fysieke beveiliging conform het Handboek Security Rijkswaterstaat uitgevoerd te hebben.

Fysieke toegangsbeveiliging
Het Systeem dient de fysieke toegangsbeveiliging van IA gerelateerde ruimten (waaronder bedien- en technische ruimten) conform paragraaf 2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimen van Cybersecurity Implementatierichtlijn Objecten – RWS.

Plaatsing en bescherming van ICT en IA
Het Systeem dient de ICT en IA tegen schade en storing beschermd te hebben.

Voedings- en telecommunicatiekabels
Het Systeem dient voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden toegepast tegen aftapping of beschadiging beschermd te hebben.

Hardening
Het Systeem dient gehardend te zijn conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van Cybersecurity Implementatierichtlijn Objecten – RWS.

Bescherming tegen malware
Het Systeem dient beschermd te zijn tegen malware conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van Cybersecurity Implementatierichtlijn Objecten – RWS.

Back-ups
Het Systeem dient de integriteit en beschikbaarheid van de ICT en IA te borgen door het maken van back-ups conform paragraaf 2.10 Maatregelen Back-ups van Cybersecurity Implementatierichtlijn Objecten – RWS.

Activiteiten in logbestanden
Het Systeem dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vastgelegd te hebben in logbestanden conform paragraaf 2.6 Maatregelen Logging en Monitoring van Cybersecurity Implementatierichtlijn Objecten – RWS.

Compartimentering infrastructuur
Het Systeem dient voor de IA gebruik te maken van een eigen gecompartimenteerde datanetwerk die van de kantoorautomatisering is afgescheiden. De scheiding kan fysiek of logisch zijn.

Segmentering van dataverkeersstromen
Het Systeem dient segmentering van dataverkeersstromen voor productie, beheer en OTA toegepast te hebben binnen de lokale objectdatanetwerken voor de IA toepassingen.

Datanetwerkverbindingen
Het Systeem dient alle datanetwerkverbindingen met het RWS datanetwerk strikt en uitsluitend gekoppeld te hebben via de centrale beveiligde voorzieningen en conform de [Nieuwe Netwerkvoorzieningen Verkeer en Waterstaat - Aansluitvoorwaarden].

Directe vaste of draadloze datanetwerkverbindingen van het Systeem met andere datanetwerken dan die van RWS zijn strikt verboden."

Minimalisatie datanetwerkkoppelingen
Het Systeem dient het aantal datanetwerkkoppelingen tussen de ICT en IA met andere externe datanetwerken te minimaliseren conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van Cybersecurity Implementatierichtlijn Objecten – RWS.

Gebruik veilige communicatie protocollen
Het Systeem dient indien het configureren van de ICT en IA-systemen van het Systeem op afstand plaatsvindt, dit over beveiligde verbindingen plaats te laten vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door de Opdrachtgever het onveilige communicatieprotocol worden ingezet, mits er een additioneel encryptie kanaal wordt toegepast (SSL, TLS, IPSEC etc.).

Webapplicaties
Het Systeem dient bij inzet van (web)applicaties de beveiliging van de in te zetten (web)applicaties opgebouwd te hebben conform de [ICT Beveiligingsrichtlijnen voor Webapplicaties – september 2015] van het Nationaal Cyber Security Centrum.

Validatie controles
Het Systeem dient ICT en IA voorzien te hebben van invoer en uitvoer validatie controles om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.

Bijlage 2 DBFM Cybersecurity management eisen

Uitgegeven door	RWS/CIV/SC
Vertrouwelijkheidsniveau	RWS Ongeclassificeerd
Datum	1 december 2015
Versie	1.0

Management topeis: Cybersecurity
De Opdrachtnemer dient gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA te voorkomen.

Cybersecurity weerstandsniveau
De Opdrachtnemer dient voor de Infrastructuur RWS de maatregelen uit de "Cybersecurity Implementatierichtlijn Objecten-RWS" behorende bij het hierna aangegeven cybersecurity weerstandsniveau uit te voeren. In alle gevallen geldt cybersecurity weerstandsniveau 1 behoudens en voor zover in de onderstaande tabel een ander cybersecurity weerstandsniveau is aangegeven voor de afzonderlijke objecten.

Noot: onder deze eis nog de volgende tabel:
Object: xx – cybersecurity weerstandsniveau xx

Cybersecurity standaarden
De Opdrachtnemer dient indien de "Cybersecurity Implementatierichtlijn Objecten-RWS" niet voorziet in maatregelen voor de invulling van de cybersecurity eisen, de NEN-ISO/IEC 27002 en de IEC 62443 te volgen.

Belegging verantwoordelijkheden
De Opdrachtnemer dient voor cybersecurity de verantwoordelijkheden op de daartoe geëigende plaatsen binnen de projectorganisatie te beleggen.

Cybersecurity inbreuken en verhoogde dreiging
Indien er sprake is van cybersecurity inbreuken of verhoogde dreiging, dient de Opdrachtnemer de richtlijn CS R03 Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging te volgen.

Evaluatie en verbetermaatregelen
De Opdrachtnemer dient ten minste jaarlijks de maatregelen voor cybersecurity te monitoren en te meten.

Risicomanagement voor Cybersecurity
De Opdrachtnemer dient ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 of gelijkwaardig te maken.

Inventarisatie en registratie van Configuration Items
De Opdrachtnemer dient alle Configuration Items (CI's) van de ICT en IA conform richtlijn CS RO6 Richtlijn registratie CI items in een configuration management database te registreren in een Configuration Management Database (CMDB) en deze actueel te houden.

Beschikbaar stellen CMDB
De Opdrachtnemer dient de informatie van de Configuration Items (CI's) zoals opgenomen in de Configuration Management Database (CMDB) beschikbaar te stellen aan andere beheer- en onderhoudsprocessen van Opdrachtgever.

Aanvaardbaar gebruik toegangsmiddelen
De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.

Classificatie en beveiliging informatie
De Opdrachtnemer dient voor de beveiliging van informatie van de Opdrachtgever en Documenten de door de Opdrachtgever aangegeven document-classificatie en bijbehorende beveiligingsmaatregelen aan te houden conform richtlijn CS R01 Richtlijn omgaan met vertrouwelijke informatie en documenten.

Bewustwording en scholing
De Opdrachtnemer dient inzake bewustwording en training van (zelfstandige) Hulppersonen, voor zover relevant voor hun functie, maatregelen te treffen conform paragraaf 2.7 Maatregelen Bewustwording en Training van de Cybersecurity Implementatierichtlijn Objecten – RWS.

Verklaring Omtrent het Gedrag (VOG)
De Opdrachtnemer dient de Werkzaamheden aan:
1. ontwerp- en constructietekeningen en constructieberekeningen en/of;
2. beveiligings- en veiligheidsdocumentatie en -instructies;

van:
   a. kunstwerken en/of;
   b. bediengebouwen en -ruimten en/of;
   c. dynamische verkeersmanagementsystemen en/of;
   d. ICT- en IA-systemen;
   e. kabels en leidingen;

dan wel de Werkzaamheden:
3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten;
4. aan ICT- en IA-systemen zelf;
5. aan kabels en leidingen;

door Hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en die over een Verklaring Omtrent het Gedrag (VOG) beschikken die gerelateerd is aan de beoogde Werkzaamheden.
In afwachting van het resultaat van de aanvraag van een VOG kan gedurende een periode van maximaal zes weken na aanvang van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende Hulppersoon.

Documentatie bediening en beheer
De Opdrachtnemer dient Documenten op te stellen en te onderhouden voor de bediening, het beheer, het onderhoud en de technische ondersteuning van ICT en IA.

Beveiliging documentatie
De Opdrachtnemer dient de Documenten met betrekking tot ICT en IA te beveiligen tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.

Geborgde wijzigingsprocedure
De Opdrachtnemer dient voor het doorvoeren van Wijzigingen aan ICT en/of IA een wijzigingsprocedure te hebben conform paragraaf 2.8 Maatregelen gecontroleerd wijzigen van de Cybersecurity Implementatierichtlijn Objecten - RWS.

Koppeling randapparatuur en bescherming tegen malware
De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en/of IA van de Opdrachtgever de richtlijn CS R02 Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS aan te houden voor bescherming tegen malware.

Back-ups en recovery proces
De Opdrachtnemer dient conform “Cybersecurity Implementatierichtlijn Objecten – paragraaf 2.10 Maatregelen Back-ups” een proces in te richten voor back-ups en recovery. Het recovery proces dient jaarlijks te worden getest.

Beschikbaar houden van logbestanden
De Opdrachtnemer dient de logbestanden van de ICT en IA beschikbaar te houden en op verzoek ter kennis te brengen van de Opdrachtgever.

Toegang geautoriseerden fysiek en logisch
De Opdrachtnemer dient inzake logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten maatregelen te treffen conform paragraaf 2.2 Maatregelen Logische Toegang van de cybersecurity Implementatierichtlijn Objecten – RWS.

Registratie toegang
De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van:
- de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten;
- de door de Opdrachtnemer aan alle (zelfstandige) hulppersonen verstrekte accounts met bijbehorende autorisatie voor de logische toegang tot ICT en IA.

Indien de Opdrachtgever of derden de fysieke of logische toegangsprocedure regelen, dient de Opdrachtnemer deze toegangsprocedure te volgen.

Wachtwoordrichtlijn
De Opdrachtnemer dient te handelen conform bijlage A Wachtwoord Richtlijn en bijlage B Factsheet Wachtwoorden van de Cybersecurity Implementatierichtlijn Objecten-RWS.

Datanetwerkkoppelingen
De Opdrachtnemer dient inzake datanetwerkkoppelingen maatregelen te treffen conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van de cybersecurity Implementatierichtlijn Objecten – RWS.

Remote access
Indien de Opdrachtnemer toegang tot ICT en/of IA op afstand (remote access) wenst, dient de Opdrachtnemer deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van Opdrachtgever te laten verlopen.

Aanvraagformulier Netwerktoegang voor Derden
Indien de Opdrachtnemer toegang tot ICT en/of IA op afstand (remote access) wenst, dient de Opdrachtnemer een aanvraag in te dienen conform de procedure beschreven in “Aanvraagformulier Netwerktoegang voor Derden” die de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.

Procedure melden en oplossen beveiligingsincidenten
De Opdrachtnemer dient een centraal meldpunt in te stellen voor de registratie en het oplossen van beveiligingsincidenten conform paragraaf 2.3 Maatregelen Beveiligingsincidenten en incident Response Plan van Cybersecurity Implementatierichtlijn Objecten – RWS.

Rapportage beveiligingsincidenten
De Opdrachtnemer dient direct aan de Opdrachtgever de beveiligingsincidenten te melden. De Opdrachtnemer dient maandelijks een rapportage te verstrekken van alle beveiligingsincidenten en van alle maatregelen die ter zake getroffen zijn.

Patchen
De Opdrachtnemer dient voor het patchen van de ICT en IA-systemen te handelen conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van de Cybersecurity Implementatierichtlijn Objecten – RWS.

Risicoanalyse en implementatieadvies spoed patches
Indien Opdrachtgever zelf melding maakt van spoed patches die niet kunnen wachten tot het eerst volgende patchmoment binnen het reguliere beheer en onderhoudsschema van Opdrachtnemer, dient Opdrachtnemer de Opdrachtgever per patch een implementatieadvies ter acceptatie voor te leggen. Daarbij gelden de volgende doorlooptijden:
- voor kritieke patches: maximaal 48 uur na melding door Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;
- voor niet kritieke patches: maximaal twee maanden na melding door de Opdrachtgever.

De Opdrachtnemer dient de patches, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren.

Bewijsmateriaal verzamelen en bewaren
De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen voor het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.

Continuïteit en herstel ICT en IA
De Opdrachtnemer dient conform richtlijn CS R04 Richtlijn continuiteitsplan maatregelen te nemen en een continuiteitsplan te ontwikkelen om voorbereid te zijn op de gevolgen van omvangrijke storingen in de ICT en IA en spoedig herstel na storingen wordt bewerkstelligd.

Testen continuïteitsplannen
De Opdrachtnemer dient minimaal jaarlijks de ontwikkelde continuïteitsplannen uit te voeren om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Jaarlijkse beproevingen
De Opdrachtnemer dient zijn medewerking te verlenen aan de beproevingen van de bediening, besturing en veiligheidsfuncties, die door de Opdrachtgever één keer per jaar worden uitgevoerd.

Cybersecurity Beveiligingsplan
De Opdrachtnemer dient een Cybersecurity Beveiligingsplan op te stellen als uitwerking van de cybersecurity eisen waarbij de inhoud ten minste de onderdelen bevat uit:
1. paragraaf 2.9 Maatregelen Beheer en Onderhoud van de Cybersecurity Implementatierichtlijn Objecten – RWS;
2. de Template cybersecurity Beveiligingsplan.

Audit en rapportage beveiligingsmaatregelen
De Opdrachtnemer dient minimaal een keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de rapportage ter kennis te brengen van de Opdrachtgever.

Wet bescherming persoonsgegevens
De Opdrachtnemer dient in het kader van de Wet bescherming persoonsgegeven de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen.

Wbp bewerkersovereenkomst
Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt dient de Opdrachtnemer een bewerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon “RWS bewerkersovereenkomst” die de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.

Videocamera’s en opslag videobeelden
Indien de Opdrachtnemer beheer en onderhoudswerkzaamheden uitvoert aan videocamera’s en/of systemen waarin camerabeelden zijn opgeslagen, dient de Opdrachtnemer de richtlijn CS R05 Richtlijn camera’s en omgang met camerabeelden van de verkeersregistratiesystemen te volgen.

Beveiliging spionage
De Opdrachtnemer dient op basis van risicoanalyse maatregelen tegen spionage te nemen zodanig dat de Documenten met betrekking tot ICT en IA, waaronder documentatie, offertes, contracten, netwerkschema's, modellen, tekeningen en berekeningen, zijn beveiligd tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.

Beveiliging van de Informatievoorziening
De Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.

Bijlage 3 Richtlijnen Cybersecurity

Inhoud

Inleiding

In dit document Bijlagen Richtlijnen Cybersecurity zijn als bijlagen de documenten opgenomen waarnaar vanuit contractteksten verwezen wordt. Het zijn op zichzelf staande documenten waar apart naar verwezen kan worden. Voor vereenvoudiging van beheer en distributie naar marktpartijen in het kader van aanbestedingen en contracten zijn alle richtlijnen in één document vervat.
Naast dit document blijft de Cybersecurity Implementatierichtlijn Objecten – RWS en de Template Cybersecurity Beveiligingsplan als apart document gehandhaafd.

CS R01 - Richtlijn omgaan met vertrouwelijke informatie en documenten

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

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

RWS Ongeclassificeerd
Deze informatie is voor iedereen toegankelijk.

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

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

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

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

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

- RWS Bedrijfsinformatie is alleen op basis van het 'need-to-know' principe toegankelijk voor de medewerkers van Rijkswaterstaat en de opdrachtnemer;
- Rijkswaterstaat en opdrachtnemer zijn vanaf het moment van ontvangst van informatie verantwoordelijk om binnen de eigen organisatie de ontsluiting en verwerking van de informatie op de afgesproken werkwijze van 'need-to-know' te verzorgen;
- Geprinte exemplaren van verwerkingen van RWS Bedrijfsinformatie dienen in afgesloten kasten bewaard te worden. Bij digitale opslag in de eigen kantooromgeving is versleuteling niet verplicht;
- De uitwisseling van RWS Bedrijfsinformatie mag via de mail onvercijferd tussen Rijkswaterstaat en de opdrachtnemer plaatsvinden. De maximale bestandsgrootte van de mailbijlagen bij RWS is 25 MB;

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

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

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

Over 7-ZIP

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

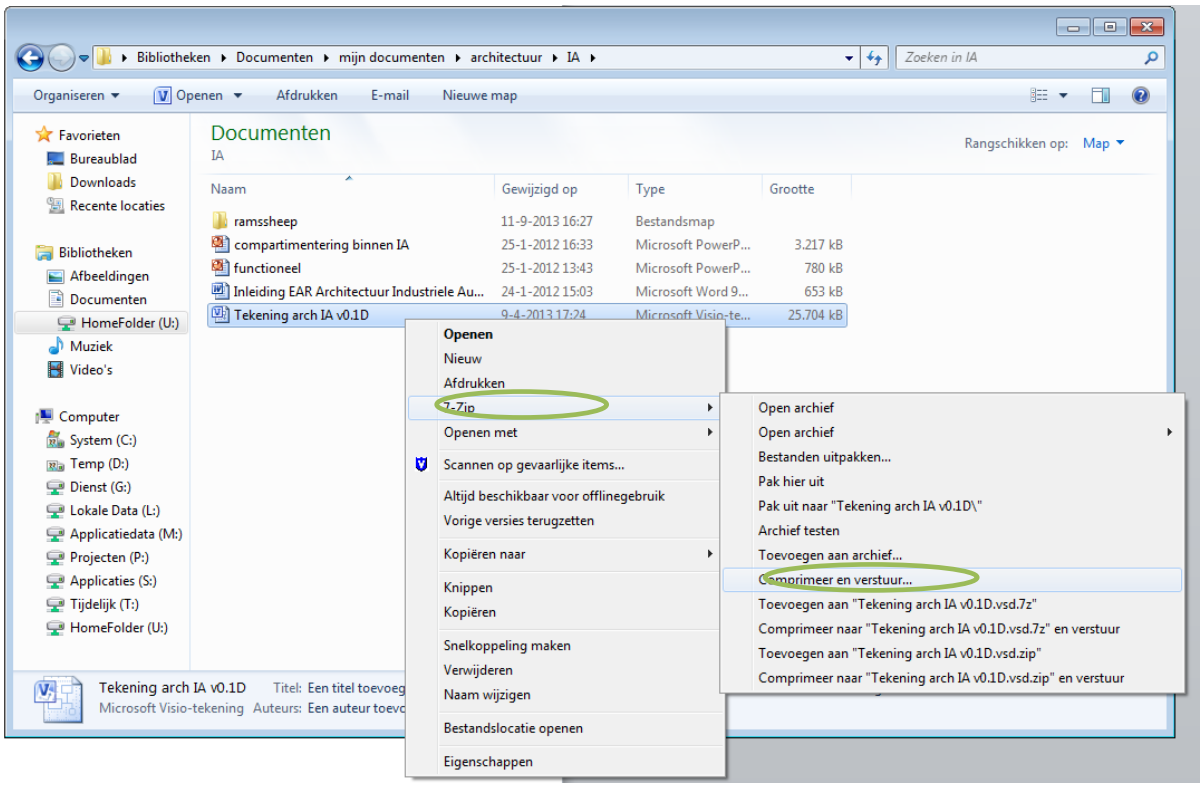
Er zijn meerdere (gratis) programma’s om bestanden in te pakken en van een wachtwoord te voorzien, maar 7-ZIP heeft een vrij sterke encryptiemethode, is standaard aanwezig op de RWS Werkplek en is tevens gratis voor (thuis)gebruik. (zie http://www.7-zip.org/).

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

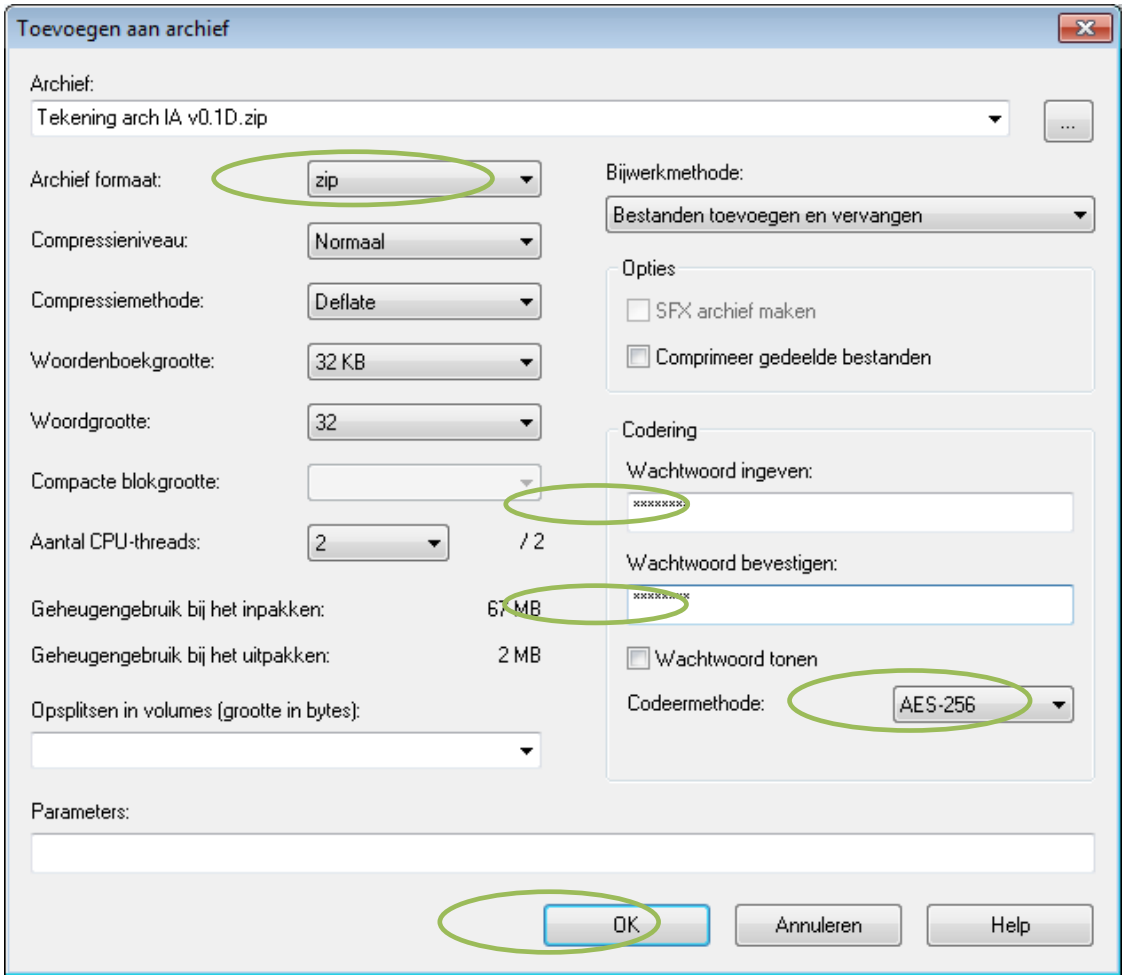
Documenten versleuteld mailen

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

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



Het volgende scherm verschijnt:



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

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

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

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

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

Je kunt meerdere bestanden of een volledige map (inclusief diens bestanden en sub-mappen) makkelijk in één keer samenvoegen.
Stap 0.
Selecteer de bestanden, die je wilt inpakken.
Stap 1.
Rechtsklik op de gekozen bestanden en/of hoofdmap en kies voor "7-Zip".
Stap 2.
Kies voor de optie uit het keuzemenu: "Toevoegen aan archief". Alle bestanden en onderliggende mappenstructuur zullen in één nieuw bestand samengebald worden.

Stap 3.
Voer in het dialoogvenster aan de rechteronderkant bij “Codering” een sterk wachtwoord in en herhaal dit wachtwoord. Standaard gebruik je hierbij AES256 versleuteling, controleer dit.

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

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

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

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

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

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

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

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

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

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

Actieve apparaten

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

Maatregelen tijdens gebruik
1. Gebruik het apparaat uitsluitend voor beheer en onderhoud van IA systemen van Rijkswaterstaat.
2. Zet 3G, 4G, WiFi en Bluetooth uit tijdens het gebruik op de objecten van RWS. (koppelingen tussen IA en andere netwerken zijn niet toegestaan)
3. Zorg vooraf voor de meest recente updates en patches van het OS van het apparaat.

4. Zorg vooraf voor de meest recente updates van de malwarescanner.
5. Download geen updates, ook niet voor ICT of IA systemen van Rijkswaterstaat, als het apparaat aan ICT of IA systemen van Rijkswaterstaat is gekoppeld. Updates en patches voor ICT of IA systemen dienen gedownload te zijn voordat de draagbare media word gekoppeld aan het ICT of IA systeem.
6. Check of downloads van ICT of IA-software uit een betrouwbare bron komen door te controleren op de meegeleverde hashcode.
7. Download ICT of IA-software uitsluitend via een beveiligde (https) verbinding.
8. Check downloads (van IA-software) op malware voordat de downloads ingezet worden binnen de ICT of IA omgeving.

Passieve apparaten (opslagmedia)

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

Bijlage A bij CS R02

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

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

Encryptie
Voor encryptie dient AES256 versleuteling te worden toegepast.

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

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

Q&A

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

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

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

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

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

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

Malware besmetting
Als (bijvoorbeeld tijdens een reguliere onderhoudsbeurt) er een (vermoeden van een) malware besmetting op het object is, dient door de monteur van de opdrachtnemer de volgende acties te worden genomen:
1. Meld een mogelijke malware besmetting op de reguliere manier als het melden van storingen onder vermelding van mogelijk risico op malwarebesmetting en geef alle bevindingen door;
2. Het oplosteam van Opdrachtgever zal contact zoeken met de monteur voor afstemming van de uit te voeren acties;
3. Wijzig niets aan het systeem als dat voor een veilige werking van het object niet strikt noodzakelijk is;
4. Maak, indien de opdrachtgever daar om vraagt conform zijn instructies, een volledige image van de (systeem)software van het betreffende IA systeem / -onderdeel;
5. Stel deze image van de (systeem)software ter beschikking aan de opdrachtgever voor nader onderzoek;
6. Wees alert op onverwachte bewegingen / storingen van het object en informeer de bedienaar om hier ook alert op te zijn;
7. Indien er (eventueel na onderzoek door de opdrachtgever) sprake blijkt te zijn van malware besmetting, controleer dan (of laat dit door de opdrachtgever doen) of de backup ook is besmet;
8. Indien er sprake is van een malwarebesmetting en de backup blijkt niet geïnfecteerd, zet dan de backup terug op het systeem;
9. Als ook de backup besmet is, zorg er dan voor dat de besmette image 'geschoond' wordt en zet de geschoonde versie terug. De opdrachtgever kan hier ondersteuning bij bieden;

10. Let op dat de juiste parameters zijn ingesteld;
11. Meld de storing op de reguliere manier af.

Verhoogde Cyberdreiging

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

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

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

De opdrachtnemer neemt de volgende acties:

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

CS R04 - Richtlijn continuiteitsplan

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

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

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

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

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

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

Doelgroep

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

Doel

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

Randvoorwaarden

Medewerkers

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

Instructies

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

1. Alleen geautoriseerde medewerkers van de opdrachtnemer mogen beheer- en onderhoudswerkzaamheden uitvoeren aan camera’s en systemen die camerabeelden opslaan;
2. De eventueel benodigde en verkregen accounts en wachtwoorden zijn strikt voor persoonlijk gebruik en mogen niet met anderen worden gedeeld. Hieronder vallen de accounts en wachtwoorden en toegangsmiddelen tot ruimten en de toegang tot de systemen binnen de ruimten;
3. Zonder uitdrukkelijke toestemming van de opdrachtgever worden camerabeelden niet vernietigd, verwijderd of verstrekt aan derden of gebruikt voor persoonlijke of bedrijfsdoeleinden;
4. Indien bestanden met camerabeelden tijdelijk opgeslagen moeten worden of een kopie gemaakt moet worden voor onderzoeksdoeleinden is zorgvuldige omgang vereist. Er dient hierbij altijd een beveiligingsmaatregel actief te zijn zodat alleen een geautoriseerde medewerker toegang kan verkrijgen tot het bestand met beelden met in achtneming van de vigerende wachtwoord policy. Voorbeeld is dat bestanden op een beveiligde usb-stick of laptop met encryptie van de harde schijf worden opgeslagen en ontsluiting via een wachtwoord plaatsvindt. Standaard dient hierbij AES-256 versleuteling gebruikt te worden;
5. Na afronding van de werkzaamheden dient controle plaats te vinden dat er geen onnodige kopieën van bestanden met camerabeelden op eigen apparatuur of media en/of back-ups achterblijft;
6. Indien onregelmatigheden worden geconstateerd rondom de inzet, werking en opslag van camerabeelden dient dit direct als beveiligingsincident bij de opdrachtgever gemeld te worden.

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

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

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

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

		Waarde	Definitie	Schrijfwijze
				gescheiden door punten.
	Configuratie		Relatie "Bestaat uit" en tegenrelatie "Is onderdeel van"	
7	**Informatie over de back-up voorziening**			
	Back-up voorziening			
8	**Datum laatste back-up en locatie van de back-up**			
	Datum laatste back-up		Datum laatste back-up	ISO 8601 formaat: jjjj-mm-dd
	Locatie van de back-up		Fysiek adres	Naam, Straat, Huisnummer, Postcode, Plaats
9	**OS (Operation System), versie OS en Firmware**			
	OS (Operation System)		Naam van de applicatie, zoals uitgegeven door de `Producent`. Indien er zowel een `Volledige naam` als een afkorting bestaat, dient hier de afkorting te worden ingevuld.	Naam van de applicatie op de box. Indien er zowel een 'Volledige naam' als een afkorting bestaat, dient hier de afkorting te worden ingevuld.
	Versie OS			
	Versie Firmware		Versie Firmware	
10	**Ingezette netwerk en applicatieprotocollen**			
	Applicatie Protocollen			LOV: SOAP, JSON,
11	**licentie informatie en verloopdatum licentie**			
	Verloopdatum licentie		De datum, waarop het contract zijn rechtsgeldigheid verliest.	ISO 8601 formaat: jjjj-mm-dd
12	**Escrow documentatie**			
	Escrow documentatie			
13	**Antimalware geïnstalleerd ja/nee**			
	Antimaleware geinstalleerd		Antimaleware geinstalleerd	LOV: Ja; Nee
14	**Welke antimalware applicatie en versie**			
	Applicatie Naam		Relatie Applicatie gebruikt Applicatie (Antimaleware)	
	Applicatie Versie		Relatie Applicatie gebruikt Applicatie (Antimaleware)	
15	**Netwerkoverzichten fysieke en logisch en IP-plan;**			
	Fysiek Netwerkoverzicht		Fysiek Netwerkoverzicht	
	Logisch netwerkoverzicht		Logisch netwerkoverzicht	
	IP-plan		IP-plan: • VICnet switch poort • Hostname RWS • Onderdeelcodering Project • Systeem Functie (bv handheld) • Source IP adres • Netwerk (bv 10.117.160.0)	

		Waarde	Definitie	Schrijfwijze
			• Subnetmask (bv 255.255.255.224) • Default Gateway (bv 10.117.160.1) • Source VLAN nummer (bv 550) • Source type (bv INTERCOM) • Ring (bv GELDW R6) • Source VPN (bv VPN-HWN :PRO-BOA) • VLAN overzicht (bv 550, DATA, VPN-VICNET:VICNET)	
16	**IP- en MAC-adres, DNS en hostnaam**			
	IP-adres		IP-adres	
	MAC-adres		Mac-adres	
	DNS		Domain Name Server Relatie "Gebruikt Server"	
	Hostnaam		Hostnaam	
17	**Documentatie patch procedure**			
	Patch documentatie			
18	**Datum laatste patch en versie**			
	Datum		Patch documentatie datum	ISO 8601 formaat: jjjj-mm-dd
	Versie		Patch versie	
19	**Vervangingsinstructie en/of – procedure voor apparaat**			
	Vervangingsinstructie en/of – procedure voor apparaat;			
20	**Identificatie en verwijzing naar vindplaats gebruikers, beheer en onderhoudsdocumentatie**			
	Identificatie			
	Verwijzing naar vindplaats gebruikers, beheer en onderhoudsdocumentatie		Verwijzing naar vindplaats gebruikers-, beheer- en onderhoudsdocumentatie	
21	**Datum laatst gewijzigd en door wie**			
	Updated		Laatst gewijzigd datum	ISO 8601 formaat: jjjj-mm-dd
	Persoon		Laatst gewijzigd door	Achternaam, Voornaam tussenvoegsel

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

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

Bijlage 4 Template - DBFM of D&C Cybersecurity Beveiligingsplan

DBFM / D&C

Cybersecurity Beveiligingsplan <20XX>

voor

<object, installatie, dienst(verlening)>

Inhoud

Inleiding

1.1 Algemeen

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

De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor. De BIR biedt een normenkader voor de beveiliging van de Informatievoorziening (IV) van het Rijk. Rijkswaterstaat 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 dreigingsprofiel dan de IV in de kantooromgeving en staan daar vaak ook los van zoals de Industriële Automatisering (IA) met veel ICS/SCADA-toepassingen.

De Cybersecurity Implementatierichtlijn Objecten - RWS is een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR en de NCSC Checklist beveiliging ICS/SCADA systemen voor de beveiliging van objecten van Rijkswaterstaat. Waar nodig zijn aanvullingen gedaan uit Best Practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen.

Tevens is in de Cybersecurity Implementatierichtlijn Objecten - RWS rekening gehouden met de risico mitigatiestrategie van Rijkswaterstaat. Primair hebben de maatregelen het doel om verstoring, misbruik en uitval binnen de IV en IA te voorkomen.

1.2 Doel

De doelstelling van dit document is om een template voor Opdrachtnemers beschikbaar te stellen waarmee de risico's met betrekking tot Cybersecurity zodanig kunnen worden beheerst dat de betrouwbaarheid (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) van de installatie, object of dienst(verlening) gedurende de looptijd van het contract wordt gewaarborgd en Cybersecurity toetsbaar wordt middels de Systeemgerichte Contract Beheersing (SCB) van Opdrachtgever.

Opdrachtnemers zijn vrij in het gebruik deze template en kunnen ook een eigen template gebruiken, mits alle informatie elementen van dit document zijn opgenomen.

1.3 Scope

Onder de scope van het Cybersecurity Beveiligingsplan vallen:
<<<<Opdrachtnemer>>>> beschrijft hier wat wel en niet onder de scope van het Cybersecurity Beveiligingsplan valt.

1.4 Doelgroep

Dit document is geschreven voor de Opdrachtnemer, beheerder van de installatie, het object of dienst(verlening) maar zal door Opdrachtgever opgevraagd en getoetst worden in het kader van de Systeemgerichte Contract Beheersing (SCB).

2. Risico's en eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS

2.1 Risico's

Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval en misbruik van ICT of de Industriële Automatisering (IA) van Rijkswaterstaat. De beheersing van de toegang of het nu fysiek of digitale vorm is, vormt letterlijk en figuurlijk het sleutelbegrip voor het terugdringen van de risico's voor de Infrastructuur van Rijkswaterstaat.

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

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

2.2 Eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS

De cybersecurity eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS die in het contract zijn opgenomen, zijn in relatie tot de scope van de opdracht en de geprioriteerde risico's door Opdrachtgever samen op basis van de door <<<< Opdrachtnemer>>>> uitgevoerde risicoanalyse en risicoafweging nader uitgewerkt in de navolgende hoofdstukken.

3. Cybersecurity beheersmaatregelen

3.1 Comply or explain

<<<<Opdrachtnemer>>>> motiveert in deze paragraaf welke Cybersecurity eisen uit het contract/overeenkomst niet of afwijkend worden ingevuld in relatie tot de scope van het Cybersecurity Beveiligingsplan, zoals beschreven in paragraaf 1.3 voor de betreffende installatie, object of dienst(verlening).

3.2 Risico's

<<<<Opdrachtnemer>>>> beschrijft hier de risico's die naar voren komen uit de periodiek door Opdrachtnemer uit te voeren risicoanalyse en risicoafweging zoals vereist in de overeenkomst of de Cybersecurity Implementatie Richtlijn Objecten RWS. De Opdrachtnemer dient voor deze installatie, object of dienst(verlening) minimaal de door Opdrachtgever in paragraaf 2.1 aangegeven risico's te mitigeren.
Indien de door Opdrachtgever aangegeven risico's niet van toepassing zijn voor het betreffende installatie, object of dienst(verlening), dan dient dit gemotiveerd te worden bij paragraaf 3.1 waar de 'comply or explain' regel geldt.

3.3 Beheersmaatregelen

Opdrachtnemer heeft voor dit object de hierna volgende Cybersecurity beheersmaatregelen getroffen die jaarlijks worden geëvalueerd en indien nodig aangepast.

3.3.1 Belegging verantwoordelijkheden

Bij <<<<Opdrachtnemer>>>> is de verantwoordelijkheid voor Cybersecurity belegd bij de <<<<afdeling/onderdeel>>>> en is <<<<de persoon>>>> voor Opdrachtgever het eerste aanspreekpunt voor Cybersecurity aangelegenheden. Bij afwezigheid zijn de vervangers bekend.

3.3.2 Borging Cybersecurity

Bij <<<<Opdrachtnemer>>>> is het beheer en onderhoud van de Cybersecurity beheersmaatregelen geborgd in zijn processen.

3.3.3 Onderaannemers

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

3.3.4 Beheer bedrijfsmiddelen en CMDB

<<<<Opdrachtnemer>>>> beschrijft conform richtlijn CS 06 op welke wijze de Configuration Items van alle ICT en IA (waaronder ICS/SCADA-systemen) worden geregistreerd in een CMDB en hoe de actualiteit van deze wordt gewaarborgd. Ook dient beschreven te worden op welke wijze deze informatie aan Opdrachtgever beschikbaar wordt gesteld.

3.3.5 Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever

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

3.3.6 Classificatie en beveiliging informatie

<<<<Opdrachtnemer>>>> beschrijft conform richtlijn CS 01 omgaan met vertrouwelijke informatie en documenten op welke wijze de beveiliging wordt bewerkstelligd van door Opdrachtgever aangegeven vertrouwelijke documenten, zoals ontwerp, constructietekeningen en datanetwerkschema's.

3.3.7 Bewustwording, scholing en VOG

<<<<Opdrachtnemer>>>> beschrijft op welke wijze het personeel bewust wordt gemaakt van de Cybersecurity risico's en aantoonbaar over de juiste opleiding, training en vaardigheden beschikt en geheimhouding in acht neemt. Voor de door Opdrachtgever aangegeven doelgroepen dient een Verklaring Omtrent het Gedrag (VOG) te worden opgenomen in de administratie.

3.3.8 Fysieke toegangsbeveiliging tot object, technische- en bedienruimten

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de fysieke toegangsbeveiliging tot de IA-gerelateerde ruimten is vormgegeven en de wijze waarop de registratie en beheer van de fysieke toegang plaatsvindt. De

registratie is actueel en kan getoetst worden door Opdrachtgever middels Systeemgerichte Contractbeheersing (SCB). In het geval dat Opdrachtgever of een derde partij het fysieke toegangsproces regelt, moet Opdrachtgever toegang via dit proces aanvragen en de spelregels naleven.

3.3.9 Logische toegangsbeveiliging tot ICT en IA-systemen

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de logische toegangsbeveiliging tot de ICT en IA-systemen is vormgegeven en de wijze waarop het account en rechtenbeheer alsmede de periodieke controles en schoning van accounts en rechten plaatsvindt. De registratie van accounts en rechten is actueel en kan getoetst worden door Opdrachtgever middels Systeemgerichte Contractbeheersing (SCB). In het geval dat Opdrachtgever of een derde partij het fysieke toegangsproces regelt, moet Opdrachtgever toegang via dit proces aanvragen en de spelregels naleven.

3.3.10 Wachtwoordrichtlijn

<<<<Opdrachtnemer>>>> beschrijft op welke wijze invulling wordt gegeven aan de door Opdrachtgever beschikbaar gestelde wachtwoordrichtlijn. Opdrachtnemer geeft gemotiveerd aan of er afwijkingen bestaan en controleert periodiek de naleving van de wachtwoord- richtlijn door zijn personeel.

3.3.11 Back-up en recovery proces

<<<<Opdrachtnemer>>>> beschrijft het back-up en recovery proces zowel qua proces als de hiervoor gebruikte voorzieningen alsmede de opslag locatie van de back-ups conform de eisen uit de overeenkomst en de Cybersecurity Implementatie Richtlijn Objecten RWS. De Opdrachtnemer test jaarlijks het recovery proces en beschrijft de resultaten ook in het hoofdstuk 7 ‘Evaluatie en actualisatie beheersmaatregelen’.

3.3.12 Beveiliging documentatie

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de bedien- , beheer en technische documentatie beschermd wordt tegen verlies en ongeautoriseerde kennisname of wijziging.

3.3.13 Wijzigingsproces

<<<<Opdrachtnemer>>>> beschrijft hier het wijzigingsproces die gevolgd wordt voor het doorvoeren van (functionele) wijzigingen aan ICT en IA conform de eisen uit de overeenkomst en de Cybersecurity Implementatie Richtlijn Objecten RWS. In voorkomende gevallen dienen security gerelateerde wijzigingen gerapporteerd en specifiek in hoofdstuk 7 te worden uitgeschreven.

3.3.14 Beveiliging tegen malware, hardening en patching

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de bescherming tegen malware wordt vormgegeven qua proces en voorzieningen alsmede de hardening en patching van ICT en IA (waaronder ICS/SCADA).

3.3.15 Patch proces en kritieke Patches

<<<<Opdrachtnemer>>>> beschrijft op welke wijze het patchproces wordt vormgegeven zowel qua proces als de hiervoor gebruikte voorzieningen en hoe de risicoafweging plaatsvindt inclusief de formulering van het advies aan Opdrachtgever conform de eisen uit de Cybersecurity Implementatie Richtlijn Objecten RWS.

3.3.16 Koppeling van apparatuur

<<<<Opdrachtnemer>>>> beschrijft conform richtlijn CS R02 veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS op welke wijze de bescherming tegen malware wordt vormgegeven qua proces en voorzieningen bij koppeling van mobiele apparatuur of removable media aan de ICT en IA (waaronder ICS/SCADA) van Opdrachtgever door Opdrachtnemer of zijn (hulp)personen.

3.3.17 Logging en monitoring

<<<<Opdrachtnemer>>>> beschrijft op welke wijze logging en monitoring wordt vormgegeven qua proces en voorzieningen in aansluiting op de eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS.

3.3.18 Datanetwerkkoppelingen

<<<<Opdrachtnemer>>>> geeft een overzicht en beschrijving van alle bestaande datanetwerkkoppelingen (met welke netwerken en partijen, doel van de koppeling en de beveiliging van de datanetwerkkoppeling) en de mate van conformiteit aan het hoofdstuk ‘Maatregelen Netwerkkoppelingen’ uit de Cybersecurity Implementatierichtlijn Objecten RWS.

3.3.19 Remote Access

<<<<Opdrachtnemer>>>> beschrijft of er sprake is van remote acces voor bediening, beheer en onderhoud van ICT en IA (waaronder ICS/SCADA) van Opdrachtgever en of dit via procedure 'Aanvraag Netwerktoegang voor derden' is verlopen. Opdrachtnemer dient in het geval van remote acces via de RAS oplossing een sluitende administratie erop na te houden over de door Opdrachtgever verstrekte tokens of andere middelen voor toegang. Alle RWS bedrijfsmiddelen moeten bij einde overeenkomst worden ingeleverd.

3.3.20 Gebruik veilige communicatieprotocollen

<<<<Opdrachtnemer>>>> beschrijft indien configuratie van de ICT en IA (waaronder ICS/SCADA) op afstand plaatsvindt op welke wijze dit vorm krijgt qua proces en voorzieningen en of dit geschiedt over beveiligde verbindingen. Hierbij dient inzet van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP te worden vermeden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door Opdrachtgever het onveilige communicatieprotocol worden ingezet mits er een additioneel encryptie kanaal wordt toegepast zoals SSL, TLS, IPSEC inclusief de vermelding van de toegepaste versie.

3.3.21 Webrichtlijnen

Indien inzet van webapplicaties voor bediening en beheer op afstand van het Systeem aan de orde is, dient <<<<Opdrachtnemer>>>> te beschrijven hoe de beveiliging van de webapplicatie is vormgegeven en in hoeverre deze voldoet aan het Security kader voor (web)applicaties van Opdrachtgever.

3.3.22 Continuïteit en herstel dienstverlening

<<<<Opdrachtnemer>>>> beschrijft conform richtlijn CS R04 continuïteitsplan welke maatregelen zijn getroffen om onderbreking van dienstverlening voor Opdrachtgever tegen te gaan voor de kritieke dienstverleningsprocessen waarmee deze beschermd worden tegen de gevolgen van omvangrijke storingen en herstel bewerkstelligd wordt.

3.3.23 Testen continuïteitsplannen

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de continuïteitsplannen periodiek worden getest en geactualiseerd.

3.3.24 Beveiliging Spionage

<<<<Opdrachtnemer>>>> beschrijft welke maatregelen er zijn getroffen om documenten, zoals offertes, contracten, netwerkschema's, constructie- en bouwtekeningen te beveiligen tegen spionage in de breedste zin des woords.

3.3.25 Beveiliging van de Informatievoorziening

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

4. Cybersecurity inbreuken en verhoogde dreiging

<<<<Opdrachtnemer>>>> beschrijft hier welk proces er is ingericht en wordt gevolgd bij Cybersecurity inbreuken (incident response proces) en bij verhoogde dreiging. De status van verhoogde dreiging wordt aangegeven door Opdrachtgever waarop Opdrachtnemer met zijn proces moet aansluiten en binnen de kaders moet handelen zoals aangegeven door Opdrachtgever.

Voor sommige objecten moet Opdrachtgever voldoen aan de meldplicht van ICT-inbreuken. Indien dit aan de orde is zal Opdrachtgever dit kenbaar maken en moet Opdrachtnemer met zijn processen hierop aansluiten.

5. Cybersecurity audit

5.1 Bevindingen

<<<<Opdrachtnemer>>>> beschrijft hier de bevindingen die voortvloeien uit de jaarlijkse audit.

5.2 Risico's

<<<<Opdrachtnemer>>>> beschrijft hier de risico's in relatie tot de bevindingen uit de voorafgaande paragraaf.

5.3 Aanbevelingen en verbetermaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de aanbevelingen en de verbetermaatregelen naar aanleiding van de bevinding en hieraan gerelateerde risico's.

6. Cybersecurity beveiligingsincidenten en rapportage

6.1 Beveiligingsincidenten

<<<<Opdrachtnemer>>>> beschrijft hier de Cybersecurity beveiligingsincidenten die conform de overeenkomst maandelijks aan Opdrachtgever zijn gerapporteerd langs de door Opdrachtgever aangereikte format en criteria. Een jaaroverzicht wordt door Opdrachtnemer opgesteld om analyse van de incidenten mogelijk te maken.

6.2 Risico's

<<<<Opdrachtnemer>>>> beschrijft hier de analyse resultaten van de Cybersecurity beveiligingsincidenten die beschreven staan in de voorgaande paragraaf.

6.3 Aanbevelingen en verbetermaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de verbetermaatregelen die reeds zijn getroffen of voortvloeien naar aanleiding van de uitgevoerde analyse uit de voorgaande paragraaf.

7. Security gerelateerde wijzigingen

7.1 Security gerelateerde wijzigingen

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

7.2 Overzicht security gerelateerde wijzigingen

<<<<Opdrachtnemer>>>> beschrijft hier de security gerelateerde wijzingen die conform de overeenkomst aan Opdrachtgever zijn gerapporteerd langs de door Opdrachtgever aangereikte format en criteria.

7.3 Analyse security gerelateerde wijzigingen en aanbevelingen

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de uitgevoerde analyse van de security gerelateerde wijzigingen en geeft aan of er aanbevelingen zijn.

8. Evaluatie en actualisatie van risico's en beheersmaatregelen

8.1 Risicoanalyse en risicoafweging

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de door Opdrachtnemer conform de eis uit de overeenkomst of de Cybersecurity Implementatierichtlijn Objecten RWS uitgevoerde risicoanalyse en de risicoafweging die is gemaakt.

8.2 Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de jaarlijkse beproevingen van het back-up en recovery proces, de continuïteitsplannen en voorzieningen en geeft aan of er verbeteringen noodzakelijk zijn.

8.3 Cybersecurity beheersmaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de verbetermaatregelen die voortvloeien uit de door hem periodiek uitgevoerde risicoanalyse en risicoafweging.

9. Verklaring Opdrachtnemer

9.1 Risicoanalyse en risicoafweging

<<<<Opdrachtnemer>>>> geeft hier een samenvatting van de jaarlijkse audit, de resultaten van de analyse van de beveiligingsincidenten, de jaarlijkse risicoanalyse en risicoafweging, de jaarlijkse audit en de evaluatie en actualisatie van het Cybersecurity Beveiligingsplan en de Cybersecurity beheersmaatregelen.

10. Bijlagen

•

10.1 Relevante bijlagen

<<<<Opdrachtnemer>>>> voegt hier de relevante bijlagen toe met een korte toelichting.

Bijlage 5 Generieke vertaling RWS maatregelen

Inhoudsopgave

Achtergrondinformatie

De maatregelen uit bijlage 2 hebben een RWS achtergrond. Hierdoor zijn deze maatregelen niet altijd generiek toepasbaar. Om deze reden is ervoor gekozen om voor al deze RWS maatregelen een generieke vertaling te maken.

Voor elk van de onderstaande 10 gebieden zijn voor de maatregelen een generieke vertaling gemaakt.

Gebieden
11. Fysieke toegangsbeveiliging IA-gerelateerde ruimten
12. Logische toegang
13. Beveiligingsincidenten en incident Response Plan
14. Netwerkkoppelingen
15. Bescherming tegen malware, hardening en patching
16. Logging en Monitoring
17. Bewustwording en Training
18. Gecontroleerd wijzigen
19. Beheer en onderhoud
20. Back-ups

Fysieke toegang

Voor de eisen aan de fysieke toegang is gebruik gemaakt van de maatregelen uit de VRKI versie 2019. De vertaling van weerstandsniveau naar de maatregelen is opgenomen in onderstaande tabel. Deze is licht gewijzigd van de tabel in de CSIR, omdat deze nog naar een oudere versie van de VRKI verwijst.

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	BK3	BK2	BK1	BK1
Compartimentering / Meeneembeperking	CO/ME3	CO/ME2	CO/ME1	CO/ME1
Inbraak-installatie / Elektronische maatregelen	EL3	EL2	EL1	EL1
Alarmering / Alarmtransmissie	AT3	AT2	AT1	AT0
Alarm opvolging / Reactie	RE3	RE2	RE1	RE0

Voor uitleg van de gebruikte afkortingen wordt verwezen naar de VRKI kaart – versie 2019

Merk op voor deze eisenset dat er niet wordt uitgegaan van 24/7 bemande gebouwen. De opdrachtgever heeft dit wel. Er dient te worden uitgezocht of alarmering en alarmopvolging dan wel noodzakelijk zijn of dat hier andere eisen van toepassing zijn.

Voor de twee meest voorkomende weerstandniveaus (2 en 3) zijn in onderstaande tabel de maatregelen uitgewerkt. Weerstandsniveau 1 en 4 zijn niet opgenomen, omdat dit zeer weinig voorkomt, en er dan vrijwel altijd maatwerk nodig is.

Weerstandniveau	Nieuw (obv VRKI 2019 maatregelen, weerstandsniveau 2)	Nieuw (obv VRKI 2019 maatregelen, weerstandsniveau 3)
Toegangsbeheer	Fysieke toegang dient verleend te worden door middel van een sleutel.	Fysieke toegang dient alleen mogelijk te zijn middels elektronische toegangspas.
Toegangsproces	Toegang dient alleen te worden 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.	Toegang dient alleen te worden 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	Opdrachtnemer dient standaard organisatorische maatregelen te nemen	Opdrachtnemer dient standaard organisatorische maatregelen te nemen met daarbij een omschrijving van de specifieke organisatorische maatregelen die zijn toegespitst op het risico voor onbedoelde fysieke toegang.
Bouwkundige maatregelen	Het gebouw dient voorzien te zijn van bouwkundige maatregelen met functionerend hang- en sluitwerk en goede kwaliteit van de gevelelementen.	Het gebouw dient een minimale inbraakwerendheid te hebben van 5 minuten conform [NEN 5096] weerstandsklasse 2 OF 3 min. inbraakwerendheid + aanvullende compartimenterende maatregelen

Compartimentering / Meeneem beperkende maatregelen	Inbraakwerende kast/safe volgens VGW kwalificaties. Alles met inbraakvertraging van 3 minuten.	Bouwkundige maatregelen zonder prestatie-eis inbraakwerendheid+ compartimenterende maatregelen met prestatie-eis 5 min. inbraakwerendheid OF geen compartimenterende maatregelen
Elektronische maatregelen	Het gebouw dient te zijn voorzien van elektronische maatregelen met niveau EL 2 conform [tabel 6.4, VRKI bijlage B].	Het gebouw dient te zijn voorzien van elektronische maatregelen met niveau EL 3 conform [tabel 6.4, VRKI bijlage B].
Alarmering	Geen eisen.	Het gebouw dient te zijn voorzien van alarmtransmissiesysteem met niveau AT3 conform [VRKI bijlage B] hoofdstuk 7.
Reactie (alarmopvolging)	Geen eisen	Opdrachtnemer dient alarmopvolging door PAC te verzorgen naar een erkende particuliere beveiligingsorganisatie. OF Alarmopvolging door PAC naar sleutelhouder(s) + technische alarmverificatie waarbij opvolging door sleutelhouder + prioriteit 1 politie

Logische toegang

In dit hoofdstuk zijn de eisen aan logische toegang opgenomen. LTPO1 betreft een eis over naleving van het logische toegangsproces. Dit is ook bevat in de inkoopvoorwaarden van de opdrachtgever in artikel 6 van de algemene inkoopvoorwaarden. Dit lijkt een betere plek voor deze eis. Verder wordt geadviseerd om criteria of beleid op te stellen voor het wel of niet toepassen van two-factor authenticatie.

Vergeleken met de CSIR is het gebruik van de rijkspas verwijderd.

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
LTPO1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.
LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot het bediening- en besturingssytseem 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.	De Opdrachtnemer dient de volgende principes voor logische toegang in acht te nemen: • de toegang voor de bestuurders tot het bediening- en besturingssytseem en overige ondersteunende ICT-systemen vindt uitsluitend op basis van het 'need to have' principe plaats; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders blijft beperkt 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, wordt uitsluitend toegestaan 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.	Opdrachtnemer dient jaarlijks de toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) te beoordelen en actualiseren.
LTPO4	De lokale logische toegang voor medewerkers tot de provinciale infrastructuur, ICT, bediening- en besturingssystemen en de centrale en locale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager aangevraagd en goedgekeurd te worden.	Opdrachtgever dient de lokale logische toegang voor medewerkers tot de provinciale infrastructuur, ICT, bediening- en besturingssystemen en de centrale en locale objectnetwerken bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager aan te vragen en goed te (laten) keuren.
LTPO5	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die de opdrachtgever hiervoor beschikbaar stelt.	Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die de opdrachtgever hiervoor beschikbaar stelt.
LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld:	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 beveiligde voorzieningen van de opdrachtgever.	· 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 beveiligde voorzieningen van de opdrachtgever.
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 de opdrachtgever.	De logische toegang dient 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 de opdrachtgever.
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 de opdrachtgever.	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 de opdrachtgever.
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.	Opdrachtnemer dient 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) te borgen in een procedure. 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.	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. Afhankelijk van de rol in de keten volgen uit deze eis andere verplichtingen.
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.	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 in versleutelde vorm of gelijkwaardig beveiligd worden uitgewisseld en opgeslagen.
LTT2	De toegang tot bediening- en besturingssystemen en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.	De toegang tot bediening- en besturingssystemen en overige ondersteunende ICT-systemen dient te zijn 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.	Het systeem dient voor bedienaars en beheerders en systemen unieke ID's te hanteren zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

Beveiligingsincidenten

Incidenten moeten snel en helder worden aangepakt. Daarvoor is het noodzakelijk dat een proces is afgesproken dat iedereen in de keten zijn verantwoordelijkheid kent. Behalve deze verantwoordelijk voorschrijven aan een opdrachtnemer dient opdrachtgever ook zijn eigen verantwoordelijkheid in dit proces helder in een plan verwoord te hebben. In de eisen hieronder wordt er van uit gegaan dat de opdrachtgever een Cybersecurityincident proces heeft en een responseplan voor CS-incidenten.

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen security incidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen moet worden geëist dat zij alle security incidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.	Opdrachtnemer dient security incidenten en zwakke plekken in de beveiliging zo snel mogelijk te melden bij de daartoe ingerichte meldpunten van opdrachtgever. Opdrachtnemer dient hiertoe een geborgde procedure te hebben voor bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen. Bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen dienen security incidenten, verdachte of zwakke plekken in systemen of diensten te registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.
BIRPO2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.	Opdrachtnemer dient een Incident Manager te benoemen en bijbehorende verantwoordelijkheden voor Cybersecurity vast te stellen.
BIRPO3	Er is bestaat een geborgde procedure voor de reactie op en eventuele escalatie van security incidenten. De security incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen.	Opdrachtnemer dient voor de reactie op en eventuele escalatie van security incidenten een procedure te hebben ingericht. De security incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, security incidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen.

BIRPO4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op die van de opdrachtgever.	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op die van de opdrachtgever.
BIRPO5	Voor het afhandelen van urgente en niet-standaard security incidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incidentmanager van de opdrachtgever ingeschakeld.	Opdrachtnemer dient de Incidentmanager van de opdrachtgever in te schakelen voor het afhandelen van urgente en niet-standaard security incidenten, zoals computervirusinfecties en aanvallen via publieke netwerken zoals internet.
BIRPO6	Er dient een geborgde procedure te bestaan voor incidentrespons ingeval van incidenten en calamiteiten.	Opdrachtnemer dient incidentrespons ingeval van incidenten en calamiteiten te borgen in een procedure.
BIRPO7	Jaarlijks dienen de incident responseplannen beproefd te worden aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van incidentresponse is het testen van de noodbediening.	Opdrachtnemer dient jaarlijks de incidentresponseplannen te beproeven aan de hand van een actueel oefenplan op doeltreffendheid. Minimaal onderdeel van incidentresponse is het testen van de noodbediening.
BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten. Toelichting: Veel systemen detecteren en loggen informatie die relevant kan zijn bij het analyseren van incidenten. Deze eis is bedoeld dat deze informatie optimaal benut wordt.

Netwerkkoppelingen

Om te kunnen bepalen wat wel en niet toegestaan is met betrekking tot netwerkkoppelingen is het van belang dat de bestaande 'Netwerkarchitectuur' bekend is en meegeleverd kan worden naar de opdrachtnemer. Geadviseerd wordt om te streven naar een eenduidige netwerkarchitectuur voor alle technische automatiseringen, zodat domeinen gebruikmaken van dezelfde architectuur. Het beleid met betrekking tot IA dient te worden opgenomen in de 'IA-kaderstelling'.

Van hieruit dient te worden bepaald wat wel en niet is toegestaan indien wordt aangesloten op het netwerk. Welke mogelijkheden biedt opdrachtgever voor remote toegang? Dit kan verwoord worden in de 'Aansluitvoorwaarden' en in de 'Beveiligingsvoorschriften', welke in de eisen ook worden aangehaald.

In vergelijking met de CSIR van RWS is hier de Producten en diensten catalogus (PDC) uitgehaald. NKPO5 gaat over hardening. Om deze eis actueel te houden adviseren wij de best practice benchmark aan te houden zoals bijvoorbeeld te vinden op https://www.cisecurity.org/cis-benchmarks/ (2019).

Specifieke documenten van opdrachtgever waarnaar gerefereerd wordt:

- Netwerkarchitectuur
- Aansluitvoorwaarden
- Beveiligingsvoorschriften
- IA-kaderstelling

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
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 de opdrachtgever(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.	Opdrachtnemer dient zorg te dragen en er op toe te zien dat netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden in overeenstemming en passend in de netwerkarchitectuur van de opdrachtgever zoals vastgelegd in … Opdrachtnemer dient in overleg met opdrachtgever waar mogelijk gebruik te maken van reeds bij opdrachtgever beschikbare generieke netwerkdiensten. Rechtstreekse toegang tot bediening- en besturingsystemen 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.	Opdrachtnemer dient zorg te dragen en er op toe te zien dat netwerkkoppelingen tussen het object en de netwerkvoorzieningen van oprachtgever voldoen aan de aansluitvoorwaarden en beveiligingsvoorschriften van opdrachtgever. Toelichting: remote logische toegang voor beheerdoeleinden verdient hierbij speciale aandacht.

NKPO3	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met de opdrachtgever voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de Netwerkarchitectuur inclusief security en de IA-kaderstelling.	Opdrachtnemer dient bij renovatie en nieuwbouw van lokale objectdatanetwerken af te stemmen met de opdrachtgever voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de Netwerkarchitectuur inclusief security en de IA-kaderstelling.
NKPO4	Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen tussen bedienin- en besturingssystemen 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.	Opdrachtnemer dient het aantal data netwerkkoppelingen tussen bediening- en besturingssystemen en andere datanetwerken beperken 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. Opdrachtnemer dient voor elke koppeling een risicoanalyse en -afweging te maken.
NKPO5	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').	Opdrachtnemer dient zorg te dragen en er op toe te zien dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen malware, hardening en patching').
NKPO6	Het koppelen van mobiele apparatuur van derden of removable media aan lokale bediening- en besturingssystemen, lokale objectdatanetwerken of het opdrachtgever-datanetwerk dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.	Opdrachtnemer dient het koppelen van mobiele apparatuur van derden of removable media aan lokale bediening- en besturingssystemen, lokale objectdatanetwerken of het datanetwerk van de opdrachtgever enkel plaats te laten vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.
NKPO7	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door middel van een Configuration Management Database (CMDB).	Opdrachtnemer dient de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken te borgen in een Configuration Management Database (CMDB).
NKPO8	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit de opdrachtgever.	Opdrachtnemer dient draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit de opdrachtgever.
NKT1	Wanneer configuratie van bediening- en besturingssystemen 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).	Configuratie van bediening- en besturingssystemen op afstand dient over beveiligde verbindingen plaats te vinden.
NKT2	Bediening- en besturingssytemen en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.	Bediening- en besturingssytemen en de ondersteunende systemen en besloten (lokale) objectnetwerken dienen geen directe verbindingen hebben met kantoornetwerken.

Malware, hardening en patching

MHPT2 vraagt van de opdrachtnemer om antimalware af te stemmen met de opdrachtgever. Is de opdrachtgever op voorhand al in staat om hier uitgangspunten over mee te geven? Dit kan de opdrachtnemer helpen met het bepalen van maatregelen.

Om deze hardening actueel te houden adviseren wij de best practice benchmark aan te houden zoals bijvoorbeeld te vinden op https://www.cisecurity.org/cis-benchmarks/ (2019).

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
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.	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 de bediening- en besturingssystemen en overige ondersteunde ICT-systemen en datanetwerkelementen door:	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van de bediening- en besturingssystemen en overige ondersteunde ICT-systemen en datanetwerkelementen door:
	• niet noodzakelijke datanetwerkservices uit te zetten;	• niet noodzakelijke datanetwerkservices uit te zetten;
	• het verwijderen (patchen) van bekende kwetsbaarheden;	• het verwijderen (patchen) van bekende kwetsbaarheden;
	• alle poorten die niet nodig zijn te deactiveren/blokkeren;	• alle poorten die niet nodig zijn te deactiveren/blokkeren;
	• alle default “access points” te verwijderen;	• alle default “access points” te verwijderen;
	• De default accounts uit te schakelen conform het wachtwoord policy;	• De default accounts uit te schakelen conform het wachtwoord policy;
	• Indien beschikbaar gebruik te maken van de security opties van leveranciers.	• Indien beschikbaar gebruik te maken van de security opties van leveranciers.
MHPPO3	De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.	De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.
MHPPO4	De Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde bediening- en besturingssystemen en ondersteunende ICT-systemen en netwerken.	De Opdrachtnemer dient tijdig te reageren op technische kwetsbaarheden van de in gebruik zijnde bediening- en besturingssystemen en ondersteunende ICT-systemen en netwerken en dit procedureel te borgen.
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.	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.	Opdrachtnemer dient patches en anti-virusupdates, die vanaf Internet worden gedownload, te controleren op contact met de juiste Internetsite en/of het verifieren van het gebruik van digitale handtekeningen van een betrouwbare certificate authority.
MHPPO7	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging schriftelijk te worden vastgelegd voorzien van een risicoafweging.	Opdrachtnemer dient, indien patches om bepaalde redenen bewust niet worden doorgevoerd, deze afweging schriftelijk vast te leggen en te voorzien van een risicoafweging.
MHPPO8	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.	Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
MHPPO9	Voor zover technisch te scannen dienen zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te worden gescand.	Opdrachtnemer dient zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te scannen.
MHPPO10	Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op malware gecontroleerd worden voordat deze worden gekoppeld aan de bediening- en besturingssysmten of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.	Opdrachtnemer dient zorg te dragen voor en erop toe te zien dat gegevensdragers, beheer- en onderhoudsapparatuur op malware gecontroleerd worden voordat deze worden gekoppeld aan de bediening- en besturingssystemen of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
MHPT1	Indien mogelijk dienen bediening- en besturingssystem zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.	Bediening- en besturingssystem dienen zodanig (her)geconfigureerd te zijn dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet is toegestaan.
MHPT2	Antimalware voorzieningen moeten in afstemming met de opdrachtgever ingezet worden.	Het systeem dient voorzien te zijn van antimalware voorzieningen. Invulling wordt in overleg met opdrachtgever bepaald.

Logging en monitoring

LMPO4 gaat over een centrale logging. In hoeverre is deze eis van toepassing voor de opdrachtgever? Ook is het de vraag of de opdrachtgever het wenselijk vindt om het verwijderen van logregels toe te staan, terwijl dit wordt opgenomen in een nieuwe logregel.

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
LMPO1	De handelingen van medewerkers, beheerders, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in auditlogbestanden 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	Opdrachtnemer dient zorg te dragen en er op toe te zien dat de handelingen van medewerkers, beheerders, meldingen vanuit andere systemen en eventlogs vastgelegd worden in auditlogbestanden 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 bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden drie maanden bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.	Opdrachtnemer dient zorg te dragen en er op toe te zien dat: • de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden drie maanden bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
LMPO3	Voor de levering van logbestanden aan derden dient de Objectverantwoordelijke/-beheerder expliciet toestemming te verlenen.	Voor de levering van logbestanden aan derden dient de 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 de opdrachtgever.	Opdrachtnemer draagt zorg voor een geborgde procedure die opvolging geeft aan meldingen uit de centrale logging en monitoringsvoorzieningen en proces vanuit de opdrachtgever.
LMPO5	Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het bediening- en besturingssystemen en gekoppelde ICTcomponenten 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.	Opdrachtnemer dient de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het bediening- en besturingssystemen en gekoppelde ICTcomponenten in kaart te brengen en te bewaken. Een geborgde procedure is aanwezig voor het bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.
LMT1	Logfiles van bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en-netwerkelementen dienen in CSV-formaat opgeleverd te kunnen worden.	Logfiles van bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en-netwerkelementen dienen in een uitwisselbaar formaat, zoals CSV, opgeleverd te 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.	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.	Het overschrijven of verwijderen van logregels- en bestanden dient te zijn gelogd in een nieuw aangelegde log.
LMT4	De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.	De loginstellingen en -bestanden dienen zodanig beschermd te zijn dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.
LMT5	Voor kritieke bediening- en besturingssystemen en overige ondersteunende ICT-systemen moet in afstemming met en op verzoek van Opdrachtgever beveiligingsspecifieke logsystemen worden ingezet.	Voor kritieke bediening- en besturingssystemen en overige ondersteunende ICT-systemen dienen in afstemming met en op verzoek van Opdrachtgever beveiligingsspecifieke logsystemen te zijn ingezet.

Maatregelen bewustwording en training

Bewustwording en training is erg specifiek voor de eigen organisatie. De eigen regels en procedures dienen herhaaldelijk te worden getraind.

Specifieke documenten van opdrachtgever waarnaar gerefereerd wordt:

- Wachtwoordrichtlijn. Indien dit document niet beschikbaar is bij de opdrachtgever kan worden teruggevallen op de wachtwoordrichtlijn van RWS.
- Cybersecurity beveiligingsinstructies

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
BTME1	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door Opdrachtgever aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, ELearning modulen te volgen en hiernaar te handelen.	Opdrachtnemer dient de door Opdrachtgever aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, ELearning 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.	Opdrachtnemer dient iedere medewerker bewust te maken van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en laten weten dat gebruikers- en systeemactiviteiten worden gelogd.
BTME3	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.	Opdrachtnemer dient de Cybersecurity beveiligingsinstructies strikt in acht te nemen en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
BTME4	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Object-beheerder.	Opdrachtnemer dient aan sociale controle te doen en personeel, medewerkers van opdrachtgever en derden aan te spreken op ontoelaatbaar en risicovol gedrag. Opdrachtnemer dient geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder te bespreken.

BTME5	Bij het constateren van een security incident dient Opdrachtnemer, bedienaar, beheerder en overig ondersteunend personeel dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het Cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen; - niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.	Opdrachtnemer dient bij het constateren van een security incident dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het Cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen; - niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.	Opdrachtnemer dient zo snel mogelijk afwijkend systeemgedrag te rapporteren als een beveiligingsincident en dit te melden aan de Objectverantwoordelijke/-beheerder, omdat dit een aanwijzing kan zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek.
BTME7	Opdrachtnemer, Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.	Opdrachtnemer dient bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties, handelingen te verrichten of maatregelen te 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.	Opdrachtnemer dient zorgvuldig om te gaan met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en deze niet te delen met collega's.
BTME9	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.	Opdrachtnemer dient geen eigen netwerkkoppelingen te creëren op het object. Opdrachtnemer dient geconstateerde verdachte netwerkkoppelingen te melden als een beveiligingsincident.
BTME10	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot bediening- en besturingssystemen en overige ondersteunende ICT-systemen in acht.	Opdrachtnemer dient de wachtwoordrichtlijn voor de logische toegang tot bediening- en besturingssystemen en overige ondersteunende ICT-systemen in acht te nemen.
BTME11	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de bediening- en besturingssystemen, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.	Opdrachtnemer dient geen mobiele apparatuur of removable media aan de bediening- en besturingssystemen, overige ondersteunende ICT-systemen en object netwerken te koppelen. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.
BTME12	Voor Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf bediening- en besturingssystemen en overige daaraan ondersteunende ICT-systemen strikt verboden.	Opdrachtnemer dient vanaf bediening- en besturingssystemen en overige daaraan ondersteunende ICT-systemen geen gebruik te maken van internet en email .
BTME13	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.	Opdrachtnemer dient de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot en ondersteunende systemen en –netwerken alleen te 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.	Opdrachtnemer dient accountgegevens strikt geheim te houden; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.
BTME15	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel dienen op bedienings- besturingssystemen en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van de opdrachtgever.	Opdrachtnemer dient op bedienings- besturingssystemen en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van opdrachtgever.
BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot bedienings- besturingssystemen en overige ondersteunende ICT-systemen dient Opdrachtnemer dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.	Bij het constateren van onregelmatigheden in de logische toegang tot bedienings- besturingssystemen en overige ondersteunende ICT-systemen dient Opdrachtnemer dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usbsticks aan het netwerk of bediening- en besturingssystemen is strikt verboden.	Opdrachtnemer dient niet ongeautoriseerd removable apparatuur of usbsticks aan het netwerk of bediening- en besturingssystemen te koppelen.
BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of bediening- en besturingssystemen systemen.	Opdrachtnemer dient zorgt te dragen en er op toe te zien dat alleen geautoriseerde medewerkers/beheerders systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of bediening- en besturingssystemen systemen.
BTME19	Gegevensdragers worden altijd vooraf op malware gecontroleerd voordat deze worden gekoppeld aan bediening- en besturingssystemen of overige ondersteunende ICT-systemen en netwerken.	Opdrachtnemer dient gegevensdragers op malware te controleren voordat deze worden gekoppeld aan bediening- en besturingssystemen 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.	Opdrachtnemer dient incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces te melden bij de Objectverantwoordelijke/ -beheerder.

BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.	Opdrachtnemer dient onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces te melden bij de Objectverantwoordelijke/ -beheerder.
BTME22	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde bediening- en besturingssystemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.	Opdrachtnemer, bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde bediening- en besturingssystemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.
BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt door Opdrachtnemer en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.	Opdrachtnemer dient bedienaars, beheerders en overig ondersteunend personeel continu bewust te maken door geschikte training en regelmatige bijscholing 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 ELearningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de bediening- en besturingssystemen en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel, objectverantwoordelijke/-beheerder	Opdrachtnemer dient zorg te dragen voor en er op toe te zien dat bedienaars, beheerders en overig ondersteunend personeel: • de periodieke Cybersecurity cursussen, trainingen en ELearningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de bediening- en besturingssystemen 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;	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 de opdrachtgever als die van externe partijen alle bedrijfsmiddelen, bediening- en besturingssystemen en overige ondersteunende ICTsysteemdocumentatie van de opdrachtgever 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 de opdrachtgever 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.	• dat bedienaars, beheerders en overig ondersteunend personeel van zowel de opdrachtgever als die van externe partijen alle bedrijfsmiddelen, bediening- en besturingssystemen en overige ondersteunende ICTsysteemdocumentatie van de opdrachtgever 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 de opdrachtgever als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.
BTMA3	De Opdrachtnemer/objectverantwoordelijke/beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.	De Opdrachtnemer dient beveiligingsincidenten van de afgelopen periode te bespreken en evalueren in de periodieke werkoverleggen. Hierbij wordt besproken 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.	Opdrachtnemer dient erop toe te zien 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.	Opdrachtnemer dient Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders bespreken en dient hiertoe opleidingsplannen te maken en dient toe te zien op de uitvoering.
BTMA6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot bediening- en besturingssystemen en overige ondersteunende ICTsystemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot bediening- en besturingssystemen en overige ondersteunende ICTsystemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord te laten wijzigen.

Gecontroleerd wijzigen

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Niew
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.	Opdrachtnemer dient alle Configuration Items (CI's) met bijbehorende settings/configuraties te registreren in een Configuration Management Database (CMDB) en deze actueel te houden.
GWPO2	Opdrachtnemer dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan bediening- en besturingssystemen en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.	Opdrachtnemer dient gecontroleerd wijzigingen door te voeren aan bediening- en besturingssystemen en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd. Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.
GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.	Opdrachtnemer dient wijzigingen alleen door geautoriseerde medewerkers te laten aanvragen en dient alleen wijzigingen in behandeling te nemen die door een geautoriseerde persoon zijn aangevraagd.
GWPO4	Voor wijzigingen aan bediening- en besturingssystemen en overige ondersteunende ICTsystemen 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.	Opdrachtnemer dient voor wijzigingen aan bediening- en besturingssystemen en overige ondersteunende ICTsystemen altijd een risicoafweging te maken als onderdeel van de impactanalyse. 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 bediening- en besturingssystemen en overige ondersteunende ICTsystemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.	Opdrachtnemer dient de wijzigingen in de CMDB bij te werken en dient jaarlijks de inhoud van de CMDB te verifieren met de settings/configuraties van bediening- en besturingssystemen en overige ondersteunende ICTsystemen en de CMDB bij afwijkingen bij te werken.
GWPO6	Wijzigingen in bediening- en besturingssystemen 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 bediening- en besturingssystemen en overige ondersteunende ICT-systemen controle worden uitgevoerd voor de authenticiteit/integriteit van de software voorafgaande aan de implementatie op operationele systemen.	Opdrachtnemer dient wijzigingen in bediening- en besturingssystemen en overige ondersteunende ICT-systemen vooraf aan de implementatie in productie te testen om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit of beveiliging van de organisatie. Bediening- en besturingssystemen en overige ondersteunende ICT-systemen dienen te zijn gecontroleerd op 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.	Opdrachtnemer dient zorg te dragen voor en er op toe te zien 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.	Opdrachtnemer dient voor elke wijziging een terugvalscenario op te stellen waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. Kort na de implementatie van een wijziging dient een test plaats te vinden om te verifiëren dat de wijziging is gelukt of dat op het terugval scenario moet worden overgegaan.
GWPO9	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.	Opdrachtnemer dient uitgeschakelde beveiligingsmaatregelen weer te activeren na een wijziging alvorens de wijziging te sluiten.
GWT1	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop dienen te zijn geregistreerd in een CMDB.
GWT2	Voor zover beschikbaar wordt gebruik gemaakt van testvoorzieningen.	Beschikbare testvoorzieningen dienen geactiveerd en benut te worden. Toelichting: Om onverwachte situaties in productie te voorkomen worden zo veel als mogelijk fouten opgespoord in de testomgeving.

Beheer en onderhoud

BOT1 heeft het over standaardproducten voor fysieke toegang. Voor het gebruik van de CSIR door de opdrachtgever is het de vraag of de opdrachtgever ook beschikt over standaardproducten voor de toegang.

Specifieke documenten van opdrachtgever waarnaar gerefereerd wordt:

- Aansluitvoorwaarden en beveiligingsvoorschriften van opdrachtgever
- Regionale calamiteitenplan

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
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.	Opdrachtnemer dient zorg te dragen voor het evalueren van risico's en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cycle management.
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 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;	Opdrachtnemer dient zorg te dragen voor en er op toe te zien 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 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 opdrachtgever 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 bediening- en besturingssystemen 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 de opdrachtgever verlopen; • Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van de opdrachtgever; • Beschreven is dat wijzigingen conform het wijzigingsproces van de opdrachtgever uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden 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 provinciale of objectnetwerken strikt verboden is.	• De procedures voor aan- en afkoppeling van apparatuur beschreven zijn; • De netwerkaansluitvoorwaarden overeengekomen zijn; • De procedure “Toegang Derden” van de opdrachtgever 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 bediening- en besturingssystemen alleen uitgevoerd mogen worden vanaf systemen die voorzien zijn van de laatste security update’s en patches en actuele viruscontroleprogrammatuur; • Beschreven is dat netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden in overeenstemming en passend in de netwerkarchitectuur van de opdrachtgever; • Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van de opdrachtgever; • Beschreven is dat wijzigingen conform het wijzigingsproces van de opdrachtgever uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden 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 provinciale 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;	Opdrachtnemer dient zorg te dragen voor en ziet er op toe dat waar nodig 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 bediening-besturingssystemen; • 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;	• 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 bediening-besturingssystemen; • 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 ICT en IA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.	Opdrachtnemer dient zorg te dragen voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICT en IA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
BOPO5	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.	Opdrachtnemer dient zorg te dragen 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.	Opdrachtnemer dient toezicht te houden 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 en ziet erop toe dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.	Opdrachtnemer dient zorg te dragen voor en er op toe te zien dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.
BOPO8	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.	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.
BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de standaard producten van de opdrachtgever.	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van de opdrachtgever als die van externe partijen tot objecten en de ruimten hierbinnen dient gebruik gemaakt te worden van de standaard producten van de opdrachtgever.
BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en de bediening- en besturingssystemen wordt gebruikt gemaakt van de standaard producten en diensten van de opdrachtgever.	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en de bediening- en besturingssystemen dient gebruik gemaakt te worden van de netwerkvoorzieningen die voldoen aan de aansluitvoorwaarden en beveiligingsvoorschriften van opdrachtgever.

Back-ups

De van toepassing zijnde eisen per weerstandsniveau zijn opgenomen in onderstaande tabel.

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

ID	Tekst CSIR (oud)	Nieuw
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.	Opdrachtnemer dient automatisch een back-up te maken van alle in het systeem aanwezige dynamische en configuratiegegevens welke 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 bediening- en besturingssystemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure:	Opdrachtnemer dient de integriteit en beschikbaarheid van de laatste drie versies van de bediening- en besturingssystemen, programmatuur en besturingssystemen te waarborgen door het maken en testen van systeemimages/back-ups, conform een geborgde procedure:
	• systeemimages/back-ups worden gemaakt vooraf en na iedere	• systeemimages/back-ups worden gemaakt vooraf en na iedere
	(functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd, met deze back-up moet men in staat zijn een volledige roll-back naar de werkende situatie terug te kunnen gaan;	(functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd, met deze back-up moet men in staat zijn een volledige roll-back naar de werkende situatie terug te kunnen gaan;
	• Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevind;	• 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 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;	• Back-ups worden bewaard tot het moment van uitdienstname van betreffend systeem;
	• Ingeval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.	• Ingeval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.

BUPO3	Er bestaan gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.	Opdrachtnemer dient een gedocumenteerde herstelprocedure en volledige en actuele registers van back-up kopieën te hebben.
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.	Opdrachtnemer dient jaarlijks herstelprocedures te controleren en te testen, 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.	Opdrachtnemer dient maandelijks de gemelde incidenten en storingsmeldingen inzake back-up te evalueren en waar nodig maatregelen te treffen.
BUT1	Benodigde voorzieningen voor het back-up en restoreproces worden in overleg met de Opdrachtgever ingevuld.	Het systeeem dient een back-up en restore-voorziening te hebben. De uitvoering wordt in overleg met de opdrachtgever bepaald.

Bijlage 6 Generieke vertaling Systeem en Managementeisen Cybersecurity van RWS

Voor opname in de programma's van eisen bij een aanbesteding door een DCO.

Referenties

[1]	Stappenplan implementatie BIO IA voor decentrale overheden	Deze uitgave is te downloaden in de Bibliotheek Verkeer en Vervoer van CROW en bij www.icentrale.nl
[2]	Cybersecurity Implementatierichtlijn Objecten – RWS	Bijlage 3 bij ref. [1]
[3]	Bijlage Richtlijnen Cybersecurity	Bijlage 4 bij ref. [1]
[4]	Template - DBFM of D&C Cybersecurity Beveiligingsplan	Bijlage 5 bij ref. [1]

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
CM1	Management topeis: Cybersecurity	Aanbieder dient gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA te voorkomen.	
CM2	Cybersecurity weerstandsniveau	Aanbieder dient voor de Infrastructuur van de DCO per type object de maatregelen uit ref. [1] uit te voeren, behorende bij het in ref. [1] aangegeven cybersecurity weerstandsniveau. In alle gevallen geldt het cybersecurity weerstandsniveau per type object zoals beschreven in ref. [1] behoudens bij de offerteaanvraag voor de Nadere Overeenkomst anders is aangegeven.	
CM3	Cybersecurity standaarden	Aanbieder dient indien ref. [1] niet voorziet in maatregelen voor de invulling van de cybersecurity eisen, de NEN-ISO/IEC 27002 en de IEC 62443 te volgen.	Met ref. [1] worden ook meest recente versies van alle documenten bedoeld waar in ref. [1] naar wordt verwezen, zoals de Cybersecurity Implementatierichtlijn Objecten – RWS.
CM4	Belegging verantwoordelijkheden	Aanbieder dient voor cybersecurity de verantwoordelijkheden op de daartoe geëigende plaatsen binnen de projectorganisatie te beleggen.	
CM5	Cybersecurity inbreuken en verhoogde dreiging	Indien er sprake is van cybersecurity inbreuken of verhoogde dreiging, dient Aanbieder de richtlijn CS R03 Richtlijn in ref. [3] voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging te volgen.	
CM6	Evaluatie en verbetermaatregelen	Aanbieder dient ten minste jaarlijks de maatregelen voor cybersecurity te monitoren en te meten.	
CM7	Risicomanagement voor Cybersecurity	Aanbieder dient ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 of gelijkwaardig te maken.	
CM8	Inventarisatie en registratie van Configuration Items	Aanbieder dient alle Configuration Items (CI's) van de ICT en IA conform richtlijn CS RO6 Richtlijn registratie CI items in ref. [3] in een configuration management database te registreren in een Configuration Management Database (CMDB) en deze actueel te houden.	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
CM9	Beschikbaar stellen CMDB	Aanbieder dient de informatie van de Configuration Items (CI's) zoals opgenomen in de Configuration Management Database (CMDB) beschikbaar te stellen aan andere beheer- en onderhoudsprocessen van DCO.	
CM10	Aanvaardbaar gebruik toegangsmiddelen	Aanbieder dient alle door de DCO beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.	
CM11	Classificatie en beveiliging informatie	Aanbieder dient voor de beveiliging van informatie van de DCO en Documenten de door de DCO aangegeven document-classificatie en bijbehorende beveiligingsmaatregelen aan te houden conform richtlijn CS R01 Richtlijn omgaan met vertrouwelijke informatie en documenten in ref. [3].	
CM12	Bewustwording en scholing	Aanbieder dient inzake bewustwording en training van (zelfstandige) Hulppersonen, voor zover relevant voor hun functie, maatregelen te treffen conform paragraaf 2.7 Maatregelen Bewustwording en Training van ref. [2].	
CM13	Verklaring Omtrent het Gedrag (VOG)	Aanbieder dient de Werkzaamheden aan: 6. ontwerp- en constructietekeningen en constructieberekeningen en/of; 7. beveiligings- en veiligheidsdocumentatie en -instructies; van: f. kunstwerken en/of; g. bediengebouwen en -ruimten en/of; h. dynamische verkeersmanagementsystemen en/of; i. ICT- en IA-systemen; j. kabels en leidingen; dan wel de Werkzaamheden: 8. binnen bedien- en technische ruimten van de hiervoor genoemde objecten; 9. aan ICT- en IA-systemen zelf; 10. aan kabels en leidingen; door Hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en die over een Verklaring Omtrent het Gedrag (VOG) beschikken die gerelateerd is aan de beoogde Werkzaamheden. In afwachting van het resultaat van de aanvraag van een VOG kan gedurende een periode van maximaal zes weken na aanvang van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende Hulppersoon.	
CM14	Documentatie bediening en beheer	Aanbieder dient Documenten op te stellen en te onderhouden voor de bediening, het beheer, het onderhoud en de technische ondersteuning van ICT en IA.	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
CM15	Beveiliging documentatie	Aanbieder dient de Documenten met betrekking tot ICT en IA te beveiligen tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.	
CM16	Geborgde wijzigingsprocedure	Aanbieder dient voor het doorvoeren van Wijzigingen aan ICT en/of IA een wijzigings-procedure te hebben conform paragraaf 2.8 Maatregelen gecontroleerd wijzigen van ref. [2].	
CM17	Koppeling randapparatuur en bescherming tegen malware	Aanbieder dient bij koppeling van randappa-ratuur aan de ICT en/of IA van de DCO de richtlijn CS R02 Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS aan te houden voor bescherming tegen malware in ref. [3].	
CM18	Back-ups en recovery proces	Aanbieder dient conform "ref. [2] – paragraaf 2.10 Maatregelen Back-ups" een proces in te richten voor back-ups en recovery. Het recovery proces dient jaarlijks te worden getest.	
CM19	Beschikbaar houden van logbestanden	Aanbieder dient de logbestanden van de ICT en IA beschikbaar te houden en op verzoek ter kennis te brengen van de DCO.	
CM20	Toegang geautoriseerden fysiek en logisch	Aanbieder dient inzake logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten maatregelen te treffen conform paragraaf 2.2 Maatregelen Logische Toegang van ref. [2].	
CM21	Registratie toegang	Aanbieder dient te zorgen voor een procedure en actuele registratie van: • de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten; • de door Aanbieder aan alle (zelfstandige) hulppersonen verstrekte accounts met bijbehorende autorisatie voor de logische toegang tot ICT en IA. Indien de DCO of derden de fysieke of logische toegangsprocedure regelen, dient Aanbieder deze toegangsprocedure te volgen.	
CM22	Wachtwoordrichtlijn	Aanbieder dient te handelen conform ref. [2]. bijlage A Wachtwoord Richtlijn en bijlage B Factsheet Wachtwoorden van ref. [2].	
CM23	Datanetwerkkoppelingen	Aanbieder dient inzake datanetwerkkoppelingen maatregelen te treffen conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van ref. [2].	
CM24	Remote access	Indien Aanbieder toegang tot ICT en/of IA op afstand (remote access) wenst, dient De Aanbieder deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van DCO te laten verlopen.	
CM25	Aanvraagformulier Netwerktoegang voor Derden	Indien Aanbieder toegang tot ICT en/of IA op afstand (remote access) wenst, dient De Aanbieder een aanvraag in te dienen conform voorschriften van DCO die de DCO na opdrachtverlening op verzoek van De Aanbieder beschikbaar stelt. Bij ontbreken van voorschriften dient Aanbieder toegang tot het	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
		netwerk af te stemmen met de DCO en hierbij te voldoen aan de afgestemde voorwaarde(n).	
CM26	Procedure melden en oplossen beveiligingsincidenten	Aanbieder dient een centraal meldpunt in te stellen voor de registratie en het oplossen van beveiligingsincidenten conform paragraaf 2.3 Maatregelen Beveiligingsincidenten en incident Response Plan van ref. [2].	
CM27	Rapportage beveiligingsincidenten	Aanbieder dient direct aan de DCO de beveiligingsincidenten te melden. De Aanbieder dient maandelijks een rapportage te verstrekken van alle beveiligingsincidenten en van alle maatregelen die ter zake getroffen zijn.	
CM28	Patchen	Aanbieder dient voor het patchen van de ICT en IA-systemen te handelen conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van ref. [2].	
CM29	Risicoanalyse en implementatieadvies spoed patches	Indien DCO zelf melding maakt van spoed patches die niet kunnen wachten tot het eerst volgende patchmoment binnen het reguliere beheer en onderhoudsschema van Opdrachtnemer, dient Opdrachtnemer de DCO per patch een implementatieadvies ter acceptatie voor te leggen. Daarbij gelden de volgende doorlooptijden: • voor kritieke patches: maximaal 48 uur na melding door DCO, gerekend vanaf de eerstvolgende werkdag; • voor niet kritieke patches: maximaal twee maanden na melding door de DCO. De Aanbieder dient de patches, na Acceptatie door de DCO van het implementatieadvies, conform het advies te implementeren.	
CM30	Bewijsmateriaal verzamelen en bewaren	Aanbieder dient in voorkomende gevallen zijn medewerking te verlenen voor het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.	
CM31	Continuïteit en herstel ICT en IA	Aanbieder dient conform richtlijn CS R04 Richtlijn continuïteitsplan in ref. [3] maatregelen te nemen en een continuïteitsplan te ontwikkelen om voorbereid te zijn op de gevolgen van omvangrijke storingen in de ICT en IA en spoedig herstel na storingen wordt bewerkstelligd.	
CM32	Testen continuïteitsplannen	De Aanbieder dient minimaal jaarlijks de ontwikkelde continuïteitsplannen uit te voeren om te bewerkstelligen dat ze actueel en doeltreffend blijven.	
CM33	Jaarlijkse beproevingen	De Aanbieder dient zijn medewerking te verlenen aan de beproevingen van de bediening, besturing en veiligheidsfuncties, die door de DCO één keer per jaar worden uitgevoerd.	
CM34	Cybersecurity Beveiligingsplan	De Opdrachtnemer dient een Cybersecurity Beveiligingsplan op te stellen als uitwerking van de cybersecurity eisen waarbij de inhoud ten minste de onderdelen bevat uit:	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
		3. paragraaf 2.9 Maatregelen Beheer en Onderhoud van ref. [2]; 4. de Template cybersecurity Beveiligingsplan (ref. [4]).	
CM35	Audit en rapportage beveiligingsmaatregelen	De Aanbieder dient minimaal een keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de rapportage ter kennis te brengen van de DCO.	
CM36	Algemene Verordening Gegevensbescherming	Aanbieder dient in het kader van de Algemene Verordening Gegevensbescherming (AVG) de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen.	
CM37	Verwerkersovereenkomst	Indien Aanbieder persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt dient De Aanbieder een verwerkers-overeenkomst af te sluiten met de DCO conform een door de DCO voorgeschreven sjabloon of anders het sjabloon uit bijlage 8 van ref. [1].	
CM38	Videocamera's en opslag videobeelden	Indien Aanbieder beheer en onderhoudswerk-zaamheden uitvoert aan videocamera's en/of systemen waarin camerabeelden zijn opgeslagen, dient Aanbieder de richtlijn CS R05 Richtlijn camera's en omgang met camera-beelden van de verkeersregistratiesystemen in ref. [3] te volgen.	
CM39	Beveiliging spionage	Aanbieder dient op basis van risicoanalyse maatregelen tegen spionage te nemen zodanig dat de Documenten met betrekking tot ICT en IA, waaronder documentatie, offertes, contracten, netwerkschema's, modellen, tekeningen en berekeningen, zijn beveiligd tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.	
CM40	Beveiliging van de Informatievoorziening	Aanbieder dient het deel van zijn informatie-voorziening dat benodigd is voor de door de DCO gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de DCO geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.	
CM41	Richtlijnen in ref. [3]	Bij verwijzing inde eisen naar de richtlijnen in ref. [3] geldt dat • Als de DCO een richtlijn heeft voor het betreffende onderdeel, dan geldt die richtlijn; • Is er geen richtlijn van de DCO, dan waar 'RWS' genoemd is in de richtlijn in ref. [3] dit lezen als DCO en de richtlijn implementeren naar letter en geest van de RWS richtlijn.	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
CS1	*Systeem topeis: Cybersecurity*	Het Systeem dient vanuit het oogpunt van Cybersecurity zodanig te worden ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.	
CS2	Cybersecurity weerstandsniveau	Het Systeem dient daar waar direct of indirect verwezen wordt naar de specifieke implementatie richtlijnen uit ref. [2] te voldoen aan het standaard cybersecurity weerstandsniveau uit ref. [1], tenzij door de DCO bij de offerte aanvraag anders is aangegeven.	
CS3	Gelaagde beveiliging	Het Systeem dient de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging uitgevoerd te hebben.	
CS4	Fysieke beveiliging	Het Systeem dient fysieke beveiliging conform het Handboek Security Rijkswaterstaat uitgevoerd te hebben. Op locaties van de DCO gelden de voorschriften van DCO. Bij ontbreken van voorschriften dient Aanbieder toegang tot het netwerk af te stemmen met de DCO en hierbij te voldoen aan de afgestemde voorwaarde(n).	
CS5	Fysieke toegangsbeveiliging	Het Systeem dient de fysieke toegangsbeveiliging van de IA gerelateerde ruimten (waaronder bedien- en technische ruimten) conform paragraaf 2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimen van ref. [2] uitgevoerd te hebben.	
CS6	Plaatsing en bescherming van ICT en IA	Het Systeem dient de ICT en IA tegen schade en storing beschermd te hebben.	
CS7	Voedings- en telecommunicatiekabels	Het Systeem dient voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden toegepast tegen aftapping of beschadiging beschermd te hebben.	
CS8	Hardening	Het Systeem dient gehardend te zijn conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van ref. [2].	
CS9	Bescherming tegen malware	Het Systeem dient beschermd te zijn tegen malware conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van ref. [2].	
CS10	Back-ups	Het Systeem dient de integriteit en beschikbaarheid van de ICT en IA te borgen door het maken van back-ups conform paragraaf 2.10 Maatregelen Back-ups van ref. [2].	
CS11	Activiteiten in logbestanden	Het Systeem dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vastgelegd te hebben in logbestanden conform paragraaf 2.6 Maatregelen Logging en Monitoring van ref. [2].	
CS12	Compartimentering infrastructuur	Het Systeem dient voor de IA gebruik te maken van een eigen gecompartimenteerde datanetwerk die van de kantoorautomatisering	

Nr.	Titel	Eis	Toelichting
Cybersecurity management eisen			
		is afgescheiden. De scheiding kan fysiek of logisch zijn.	
CS13	Segmentering van dataverkeersstromen	Het Systeem dient segmentering van dataverkeersstromen voor productie, beheer en OTA toegepast te hebben binnen de lokale objectdatanetwerken voor de IA toepassingen.	
CS14	Datanetwerkverbindingen	Het Systeem dient alle datanetwerkverbindingen met het DCO-datanetwerk strikt en uitsluitend gekoppeld te hebben via de centrale beveiligde voorzieningen en conform de door de DCO voorgeschreven procedures en maatregelen. Directe vaste of draadloze datanetwerkverbindingen van Het Systeem met andere datanetwerken dan die van DCO zijn niet toegestaan.	
CS15	Minimalisatie datanetwerkkoppelingen	Het Systeem dient het aantal datanetwerkkoppelingen tussen de ICT en IA met andere externe datanetwerken te minimaliseren conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van ref. [2].	
CS16	Gebruik veilige communicatie protocollen	Het Systeem dient indien het configureren van de ICT en IA-systemen van Het Systeem op afstand plaatsvindt, dit over beveiligde verbindingen plaats te laten vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient vermeden te worden. Indien Het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door de DCO het onveilige communicatieprotocol worden ingezet, mits er een additioneel encryptie kanaal wordt toegepast (SSL, TLS, IPSEC etc.).	
CS17	Webapplicaties	Het Systeem dient bij inzet van (web)applicaties de beveiliging van de in te zetten (web)applicaties opgebouwd te hebben conform de [ICT Beveiligingsrichtlijnen voor Webapplicaties – september 2015] van het Nationaal Cyber Security Centrum.	
CS18	Validatie controles	Het Systeem dient ICT en IA voorzien te hebben van invoer en uitvoer validatie controles om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.	

Bijlage 7 Verwerkersovereenkomst

Deze verwerkersovereenkomst is opgesteld i.o.v. het Ministerie van Infrastructuur en Waterstaat t.b.v. gebruik door gemeenten, provincies en Rijkswaterstaat i.r.t. het programma Talking Traffic.

Disclaimer: opties zijn weergegeven tussen haken, deze zijn niet uitputtend, maar moeten worden gezien als voorbeelden.

Voorbeeld Verwerkersovereenkomst
Organisatie ingeschreven bij de Kamer van Koophandel onder nummer ..... statutair gevestigd te ..... en kantoorhoudende aan ....., ten deze rechtsgeldig vertegenwoordigd door ....., hierna te noemen de "**Verwerkingsverantwoordelijke**"

en

[organisatie] ingeschreven bij de Kamer van Koophandel onder nummer ..... en statutair gevestigd te ..... en kantoorhoudende aan ..... te ..... , ten deze rechtsgeldig vertegenwoordigd door ....., hierna te noemen "**Verwerker**",

Gezamenlijk aan te duiden als Partijen;

Overwegende dat:

a) Verwerkingsverantwoordelijke [optie: een wegbeheerder is] en in dat kader persoonsgegevens verwerkt;
b) Verwerker [optie: een IT-leverancier, een softwareontwikkelaar, een onderzoeksbureau];
c) Partijen in dat kader op [datum hoofdovereenkomst] een overeenkomst hebben gesloten onder de titel [titel hoofdovereenkomst] (hierna: Hoofdovereenkomst);
d) Partijen het voorzienbaar achten dat Verwerker bij de uitvoering van de Hoofdovereenkomst Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke zal Verwerken respectievelijk potentieel toegang zal hebben tot Persoonsgegevens die onder de verantwoordelijkheid van Verwerkingsverantwoordelijke vallen;
e) Partijen hun onderlinge verhoudingen ten aanzien van de (potentieel) te Verwerken Persoonsgegevens wensen vast te leggen in deze Verwerkersovereenkomst;

verklaren te zijn overeengekomen een Verwerkersovereenkomst als bedoeld in artikel 28, derde lid, van de Algemene Verordening Gegevensbescherming (hierna: AVG), tussen de Verwerkingsverantwoordelijke en de Verwerker.

Artikel 1 Definities

1.1 Betrokkene: betrokkene zoals gedefinieerd in artikel 4 AVG.
1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze Verwerkersovereenkomst.
1.3 Normen en standaarden: de door de verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de Verwerker zullen worden gevolgd als vastgelegd in Bijlage 1.
1.4 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder in de zin van artikel 51 AVG is aangesteld voor het toezicht op het verwerken van persoonsgegevens.
1.4. (Verwerkings)verantwoordelijke: de verwerkingsverantwoordelijke zoals gedefinieerd in artikel 4 AVG.
1.5. Verwerker: de verwerker zoals gedefinieerd in artikel 4 AVG. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de Verwerker, is een sub-Verwerker.
1.6. Verwerken: verwerken zoals gedefinieerd in artikel 4 AVG.
1.7. Persoonsgegevens: persoonsgegevens zoals gedefinieerd in artikel 4 AVG.

Artikel 2 Ingangsdatum en duur

2.1 Deze Verwerkersovereenkomst gaat in op het moment van [opties: ondertekening/eerste feitelijke Verwerking in het kader van de Hoofdovereenkomst] en duurt voort zolang de Verwerker als Verwerker van Persoonsgegevens optreedt in het kader van de door de Verwerkingsverant-woordelijke ter beschikking gestelde Persoonsgegevens voor het leveren van de diensten uit hoofde van de Hoofdovereenkomst.

2.2 De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Hoofdovereenkomst, of indien langer, de duur van de feitelijke Verwerking van Persoonsgegevens.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

3.1 De Verwerker Verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst. De door de Verwerker uit te voeren werkzaamheden waar deze Verwerkersovereenkomst betrekking op heeft, worden nader omschreven in Bijlage 2. Verwerker zal de persoonsgegevens niet voor enig ander doel Verwerken, behoudens afwijkende wettelijke verplichtingen (in welk geval hij zelfstandig verwerkingsverantwoordelijke in de zin van art. 4 AVG wordt) of voor het opvolgen van instructies van de Verwerkingsverantwoordelijke. De Verwerker verbindt zich om in het kader van die werkzaamheden de door of via de Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens zorgvuldig te Verwerken.

Artikel 4 Verplichtingen Verwerker

4.1 Verwerker Verwerkt Persoonsgegevens, in overeenstemming met de instructies van Verwerkingsverantwoordelijke.

4.2 De Verwerker heeft geen zeggenschap over de Verwerkte Persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van de Persoonsgegevens.

4.3 De Verwerker zal bij de Verwerking van Persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de in Nederland toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens.

4.4 De Verwerker zal te allen tijde op eerste verzoek van de contactpersoon, als bedoeld in artikel 12.2, door Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze Verwerkersovereenkomst ter hand stellen.

4.5 De Verwerker stelt de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

4.6 In het geval dat een Betrokkene een verzoek tot inzage, verbetering, aanvulling, verwijdering of afscherming van zijn of haar Persoonsgegevens, richt aan de Verwerker, zal de Verwerker het verzoek uiterlijk binnen een week door sturen aan Verwerkersverantwoordelijke.

4.7 De Verwerker werkt op verzoek van Verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffectbeoordeling (GEB), ook wel Privacy Impact Assesment (PIA) genoemd.

4.8 De door Verwerker gemaakte redelijke kosten voor een dergelijke beoordeling zijn voor rekening van de Verantwoordelijke voor zover deze activiteiten van Verwerker vergen die verder strekken dan de uit de Hoofdovereenkomst voortvloeiende informatieverplichtingen van Verwerker aan Verwerkingsverantwoordelijke .

Artikel 5 Geheimhoudingsplicht

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker, evenals de Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de Persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de Verwerker tekenen hiertoe een geheimhoudingsverklaring. Laatstgenoemde geheimhoudingsverklaring valt onder het controlerecht van artikel 7.

Artikel 6 Meldplicht datalekken en beveiligingsincidenten

6.1 De Verwerker zal de Verwerkingsverantwoordelijke zo spoedig mogelijk – doch uiterlijk binnen 36 uur na de eerste ontdekking – informeren over alle (vermoedelijke) inbreuken op de beveiliging van de Persoonsgegevens en/of gebeurtenissen die tot een (vermoedelijke) onrechtmatige Verwerking van de Persoonsgegevens heeft geleid, alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de bevoegde toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.

6.2 De Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken. De meldingsprocedure is als bijlage opgenomen bij deze Verwerkersovereenkomst. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.

6.3 De Verwerker zal het doen van meldingen aan de bevoegde toezichthouder(s) overlaten aan de Verwerkingsverantwoordelijke.

6.4 De Verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of

betrokkene(n). Daarbij verschaft Verwerker in ieder geval de informatie, zoals beschreven in Bijlage 3, aan de Verwerkingsverantwoordelijke.

6.5 De Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in Bijlage 3 is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

Artikel 7 Beveiligingsmaatregelen en controle

7.1 De Verwerker neemt alle passende technische en organisatorische maatregelen om de Persoonsgegevens welke worden Verwerkt ten dienste van de Verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige Verwerking. De wijze van beveiliging wordt nader omschreven in Bijlage 4.

7.2 De Verantwoordelijke is gedurende de looptijd van de Overeenkomsten gerechtigd om periodiek of indien omstandigheden hiertoe aanleiding geven, de Verwerking van persoonsgegevens te (doen) controleren. De Verwerker is verplicht de Verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van Verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

7.3 De Verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Verwerker, tenzij dit redelijkerwijze niet van hem gevergd kan worden. Hiervoorgaande meldingsplicht kan naar zijn aard niet afdoen aan de controlerechten van de Autoriteit Persoonsgegevens.

7.4 De Verwerker verbindt zich om binnen een door de Verwerkingsverantwoordelijke te bepalen termijn de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de Verwerker van deze Verwerkersovereenkomst. De Verwerkingsverantwoordelijke, of de door de Verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen en domeinkennis van verkeersregelingsinstallaties te hebben.

7.5 Verwerker staat ervoor in, de door de Verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren. Indien de door Verwerkingsverantwoordelijke gevergde verbeteringen in zwaarte en reikwijdte de voor wegbeheerders gangbare, en/of de door de Autoriteit Persoonsgegevens gevergde, beveiligings- en continuïteitsmaatregelen substantieel overstijgen is Verwerker gerechtigd a) de redelijke kosten hiervan in rekening te brengen aan Verwerkingsverantwoordelijke of, naar zijn keuze, b) de Hoofdovereenkomst te beëindigen in het geval Partijen ook na overleg geen overeenstemming kunnen bereiken over de gevergde maatregelen.

7.6 De Verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze Verwerkersovereenkomst. De met de rapportage gemoeide kosten zijn voor rekening van de Verwerker.

7.7 Naast rapportages door de Verwerker en controles door de Verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

7.8 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de Verwerker enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de Verwerker.

Artikel 8 Inschakeling derden

8.1 De Verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de Verwerkingsverantwoordelijke.

8.2 De Verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze Verwerkersovereenkomst.

8.3 De Verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst. De Verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de Verwerkingsverantwoordelijke en de Verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.

8.4 Doorgifte naar andere landen dan lidstaten van de Europese Economische Ruimte (EER) of Zwitserland is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

8.5 De Verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de Verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als Bijlage 5 aan deze Verwerkersovereenkomst worden toegevoegd en zal door de Verwerker actueel worden gehouden.

Artikel 9 Wijziging en beëindigen Verwerkersovereenkomst

9.1 Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.

9.2 Zodra de samenwerking is beëindigd, zal de Verwerker naar keuze van de Verwerkingsverantwoordelijke:

a) alle of een door Verwerkingsverantwoordelijke bepaald gedeelte van hem in het kader van deze Verwerkersovereenkomst ter beschikking gestelde Persoonsgegevens aan de Verwerkingsverantwoordelijke ter beschikking stellen;

b) de Persoonsgegevens die hij van of wegens de Verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij Partijen iets anders overeenkomen.

De Verwerkingsverantwoordelijke kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt. De kosten gemoeid met deze inspanningen komen voor rekening van Verwerkingsverantwoordelijke, voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van opdrachtnemer voortvloeiende uit de uitvoering van de overeenkomst.

9.3 De Verwerker zal te allen tijde de in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de Persoonsgegevens.

9.4 Verwerkingsverantwoordelijke en Verwerker treden met elkaar in overleg over wijzigingen in deze Verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

9.5 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij hem in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

9.6 Indien de Verwerkersovereenkomst voortijdig wordt beëindigd is artikel 9 lid 2 en 3 van overeenkomstige toepassing

9.7 Het beëindigen of aflopen van deze Verwerkersovereenkomst zal Verwerker niet ontslaan van zijn geheimhoudingsplicht ingevolge artikel 5.

Artikel 10 Aansprakelijkheid

10.1 De aansprakelijkheid (voor toerekenbare schade en boetes) van Partijen wordt beheerst door de bepalingen daarover in de Hoofdovereenkomst waarbij eventuele aansprakelijkheidsbeperkingen worden doorbroken in geval van opzet of grove schuld c.q. roekeloosheid.

10.2 Binnen de aansprakelijkheidsbeperkingen zoals bedoeld in artikel 10.1 vrijwaart Verwerker Verwerkingsverantwoordelijke voor schade of nadeel voor zover toe te rekenen aan de Verwerker.

10.3 Binnen de aansprakelijkheidsbeperkingen zoals bedoeld in artikel 10.1 vrijwaart Verwerkingsverantwoordelijke Verwerker voor schade of nadeel voor zover toe te rekenen aan Verwerkingsverantwoordelijke.

10.4 Hiervoorgaande vrijwaringen worden in het geval het nadeel of schade bestaat uit een opgelegde bestuurlijke boete eerst inroepbaar nadat de partij die de boete opgelegd heeft gekregen alle mogelijkheden tot bezwaar en beroep tegen de boeteoplegging heeft uitgeput, waarbij vrijwarende Partij de gevrijwaarde Partij op eigen kosten zal ondersteunen bij dergelijke bezwaar- en beroepschriftprocedures.

Artikel 11 Toepasselijk recht

11.1 Op deze Verwerkersovereenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Artikel 12 Overige bepalingen

12.1 Deze Verwerkersovereenkomst kan worden aangehaald als 'Verwerkersovereenkomst *[naam]*"

Aldus opgemaakt op:

Ondertekend te [PLAATS] Ondertekend te [PLAATS]

[DATUM DD/MMM] 2019 [DATUM DD/MMM] 2019

_____ _____

Handtekening Opdrachtgever Handtekening Opdrachtnemer

Colofon

Stappenplan implementatie BIO IA voor decentrale overheden – Handreiking voor gemeenten en provincies om te voldoen aan de Baseline Informatiebeveiliging Overheid voor Industriële automatisering

uitgave

CROW

tekst

Paul Oost, KienIA Industriële Automatisering B.V.
Gijs Withagen, KienIA Industriële Automatisering B.V.
Eelco Banis, KienIA Industriële Automatisering B.V.

eindredactie

CROW

productie

CROW

bestellen

Deze uitgave is te downloaden bij https://www.crow.nl/thema-s/verkeersmanagement/icentrale en bij https://www.icentrale.nl/kennis.

kennisplatform CROW