

DBFM / D&C

Cybersecurity Beveiligingsplan <20XX>

voor

<object, installatie, dienst(verlening)>

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

Colofon

Uitgegeven door RWS/CIV/IRN/Security Centre

Informatie

Opmaak

Datum 6 oktober 2015

Versienummer 1.0

Inhoud

1.	Inleiding	5
1.1	Algemeen.....	5
1.2	Doel	5
1.3	Scope	5
1.4	Doelgroep	5
2.	Risico's en eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS...	6
2.1	Risico's	6
2.2	Eisen uit de Cybersecurity Implementatierichtlijn Objecten RWS	6
3.	Cybersecurity beheersmaatregelen	7
3.1	Comply or explain	7
3.2	Risico's	7
3.3	Beheersmaatregelen.....	7
3.3.1	Belegging verantwoordelijkheden	7
3.3.2	Borging Cybersecurity	7
3.3.3	Onderaannemers	7
3.3.4	Beheer bedrijfsmiddelen en CMDB	7
3.3.5	Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever	7
3.3.6	Classificatie en beveiliging informatie	7
3.3.7	Bewustwording, scholing en VOG	8
3.3.8	Fysieke toegangsbeveiliging tot object, technische- en bedienruimten ...	8
3.3.9	Logische toegangsbeveiliging tot ICT en IA-systemen.....	8
3.3.10	Wachtwoordrichtlijn.....	8
3.3.11	Back-up en recovery proces.....	8
3.3.12	Beveiliging documentatie	8
3.3.13	Wijzigingsproces	8
3.3.14	Beveiliging tegen malware, hardening en patching	8
3.3.15	Patch proces en kritieke Patches	9
3.3.16	Koppeling van apparatuur	9
3.3.17	Logging en monitoring	9
3.3.18	Datanetwerkkoppelingen	9
3.3.19	Remote Access	9
3.3.20	Gebruik veilige communicatieprotocollen.....	9
3.3.21	Webrichtlijnen	9
3.3.22	Continuïteit en herstel dienstverlening	9
3.3.23	Testen continuïteitsplannen	10
3.3.24	Beveiliging Spionage.....	10
3.3.25	Beveiliging van de Informatievoorziening	10
4.	Cybersecurity inbreuken en verhoogde dreiging	11
5.	Cybersecurity audit	12
5.1	Bevindingen	12
5.2	Risico's	12
5.3	Aanbevelingen en verbetermaatregelen	12
6.	Cybersecurity beveiligingsincidenten en rapportage	13
6.1	Beveiligingsincidenten	13
6.2	Risico's	13
6.3	Aanbevelingen en verbetermaatregelen	13
7.	Security gerelateerde wijzigingen	14

7.1	Security gerelateerde wijzigingen.....	14
7.2	Overzicht security gerelateerde wijzigingen	14
7.3	Analyse security gerelateerde wijzigingen en aanbevelingen	14
8.	Evaluatie en actualisatie van risico's en beheersmaatregelen	15
8.1	Risicoanalyse en risicoafweging.....	15
8.2	Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen 15	
8.3	Cybersecurity beheersmaatregelen.....	15
9.	Verklaring Opdrachtnemer.....	16
9.1	Risicoanalyse en risicoafweging.....	16
10.	Bijlagen	17
10.1	Relevante bijlagen.....	17
11.	Begrippenlijst	18

1. 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 wijzigingen 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 Netwerktogang 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 wijzigingen 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.

11. 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).

Informatie- en Communicatietechnologie (ICT)

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

Industrial Control Systems (ICS)

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

Supervisory Control And Data Acquisition (SCADA)

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

RWS Infrastructuur

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