Cybersecurity Beveiligingsplan / Cybersecurity Dossier [20XX]

voor

[beheerobject(en)]





|  |  |
| --- | --- |
| Opdrachtnemer/Uitvoerder |  |
| **Naam** |  |
| **Functie** |  |
| **Datum**  |  |
| **Status** |  |
| **Classificatie** | Vertrouwelijk (*na invulling door ON*)  |
| **Paraaf** |  |

**Colofon**

|  |  |
| --- | --- |
| Uitgegeven door | RWS/CIV/IRN/Security Centre en het Waterschapshuis |
| Informatie |  |
| Opmaak |  |
| Datum | 10 september 2021 |
|  |  |
| Versienummer | 3.4 CONCEPT |

Inhoud

[Toelichting op het gebruik van dit template 5](#_Toc82118426)

[Algemeen 5](#_Toc82118427)

[Doelgroep 5](#_Toc82118428)

[Doelstelling 5](#_Toc82118429)

[1 Risico’s en eisen uit de Cybersecurity Implementatierichtlijn Objecten 7](#_Toc82118430)

[1.1 Risico’s 7](#_Toc82118431)

[1.2 Eisen uit de Cybersecurity Implementatierichtlijn Objecten 7](#_Toc82118432)

[2 Cybersecurity beheersmaatregelen 9](#_Toc82118433)

[2.1 Objecten en weerstandsniveau 9](#_Toc82118434)

[2.2 Scope 9](#_Toc82118435)

[2.2.1 Binnen scope 9](#_Toc82118436)

[2.2.2 Buiten scope 9](#_Toc82118437)

[2.3 Comply or explain 10](#_Toc82118438)

[2.4 Risico’s 10](#_Toc82118439)

[2.5 Beheersmaatregelen 10](#_Toc82118440)

[2.5.1 Cybersecurity aanpak, standaarden en beheersmaatregelen 10](#_Toc82118441)

[2.5.2 Belegging verantwoordelijkheden 10](#_Toc82118442)

[2.5.3 Borging Cybersecurity 11](#_Toc82118443)

[2.5.4 Onderaannemers 11](#_Toc82118444)

[2.5.5 Beheer bedrijfsmiddelen en CMDB 12](#_Toc82118445)

[2.5.6 Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever 12](#_Toc82118446)

[2.5.7 Classificatie en beveiliging informatie 13](#_Toc82118447)

[2.5.8 Bewustwording, scholing en VOG 13](#_Toc82118448)

[2.5.9 Fysieke (toegangs)beveiliging tot object, technische- en bedienruimten 14](#_Toc82118449)

[2.5.10 Logische toegangsbeveiliging tot ICT en IA-systemen 14](#_Toc82118450)

[2.5.11 Wachtwoordrichtlijn 15](#_Toc82118451)

[2.5.12 Back-up en recovery proces 15](#_Toc82118452)

[2.5.13 Documentatie bediening en beheer 16](#_Toc82118453)

[2.5.14 Beveiliging documentatie 16](#_Toc82118454)

[2.5.15 Ontwikkeling, onderhoud en wijzigingsproces 16](#_Toc82118455)

[2.5.16 Beveiliging tegen malware, hardening en patching 17](#_Toc82118456)

[2.5.17 Patch proces en kritieke Patches 18](#_Toc82118457)

[2.5.18 Koppeling van apparatuur 18](#_Toc82118458)

[2.5.19 Logging en monitoring 19](#_Toc82118459)

[2.5.20 Bewijsmateriaal verzamelen en bewaren 19](#_Toc82118460)

[2.5.21 Datanetwerkinrichting en datanetwerkkoppelingen 19](#_Toc82118461)

[2.5.22 Remote Access 20](#_Toc82118462)

[2.5.23 Gebruik veilige communicatieprotocollen en draadloze netwerken 20](#_Toc82118463)

[2.5.24 Applicaties ontwikkeling en onderhoud 21](#_Toc82118464)

[2.5.25 Continuïteit en herstel dienstverlening 22](#_Toc82118465)

[2.5.26 Periodieke beproevingen 23](#_Toc82118466)

[2.5.27 AVG en verwerkersovereenkomst 23](#_Toc82118467)

[2.5.28 Videocamera’s en opslag videobeelden 24](#_Toc82118468)

[2.5.29 Beveiliging Spionage 24](#_Toc82118469)

[2.5.30 Beveiliging van de Informatievoorziening 24](#_Toc82118470)

[2.5.31 Cybersecurity wet- en regelgeving 24](#_Toc82118471)

[2.5.32 Gelaagde beveiliging 25](#_Toc82118472)

[2.5.33 Plaatsing en bescherming van ICT en IA 25](#_Toc82118473)

[2.5.34 Voedings- en communicatiekabels 25](#_Toc82118474)

[2.5.35 Validatie controles 25](#_Toc82118475)

[3 Incidentproces, SOC meldingen en verhoogde dreiging en Recovery 26](#_Toc82118476)

[4 Cybersecurity audit 27](#_Toc82118477)

[4.1 Bevindingen 27](#_Toc82118478)

[4.2 Risico’s 27](#_Toc82118479)

[4.3 Aanbevelingen en verbetermaatregelen 27](#_Toc82118480)

[5 Cybersecurity Incident Response- en rapportageproces 28](#_Toc82118481)

[5.1 Beveiligingsincidenten 28](#_Toc82118482)

[5.2 Risico’s 28](#_Toc82118483)

[5.3 Aanbevelingen en verbetermaatregelen 28](#_Toc82118484)

[6 Security gerelateerde wijzigingen 29](#_Toc82118485)

[6.1 Security gerelateerde wijzigingen 29](#_Toc82118486)

[6.2 Overzicht security gerelateerde wijzigingen 29](#_Toc82118487)

[6.3 Analyse security gerelateerde wijzigingen en aanbevelingen 29](#_Toc82118488)

[7 Evaluatie en actualisatie van risico’s en beheersmaatregelen 30](#_Toc82118489)

[7.1 Risicoanalyse en risicoafweging 30](#_Toc82118490)

[7.2 Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen 30](#_Toc82118491)

[7.3 Cybersecurity beheersmaatregelen 30](#_Toc82118492)

[8 Verklaring Opdrachtnemer 31](#_Toc82118493)

[8.1 Risicoanalyse en risicoafweging 31](#_Toc82118494)

[9 Bijlagen 32](#_Toc82118495)

[9.1 Relevante bijlagen 32](#_Toc82118496)

# **Toelichting op het gebruik van dit template**

## Algemeen

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

De Baseline Informatiebeveiliging Overheid (BIO) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor. De BIO biedt een normenkader voor de beveiliging van de Informatievoorziening (IV) van de overheid. Maar er zijn ook veel systemen en omgevingen die los staan van de IV 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. Proces Automatisering (PA) is een synoniem van Industriële Automatisering (IA).

De Cybersecurity Implementatierichtlijn Objecten (CSIR) is een vertaalslag en specifieke invulling van de relevante beheersdoelen/controls en maatregelen uit de BIO en de IEC 62443[[1]](#footnote-1), voor de beveiliging van objecten en andere omgevingen die die los staan van de IV systemen. Waar nodig zijn aanvullingen gedaan uit Best Practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen.

Primair hebben de maatregelen in de CSIR het doel om verstoring, misbruik en uitval binnen de IV en IA te voorkomen.

## 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 conform de vereisten zoals vermeld in het contract.

## Doelstelling

Dit document fungeert als template voor Opdrachtnemers om te beschrijven op welke wijze zij invulling geven aan de gestelde eisen omtrent cybersecurity voor het object, installatie of dienst(verlening). Het document dient inzichtelijk te maken op welke wijze de risico’s met betrekking tot cybersecurity worden beheerst, zodat dat de betrouwbaarheid van de objectfuncties, de veiligheid en continuïteit gedurende de looptijd van het contract wordt gewaarborgd. Op deze wijze wordt cybersecurity toetsbaar door de Opdrachtgever.

**Invullen**

In dit template staan op een aantal plaatsen blokhaken […]. Tussen de blokhaken staat in HOOFDLETTERS beschreven wat Opdrachtnemer daar dient in te vullen. Zo dient Opdrachtnemer bij [OPDRACHTNEMER][[2]](#footnote-2) de eigen bedrijfsnaam in te vullen, en bij [BESCHRIJF SCOPE][[3]](#footnote-3) de scope van het Cybersecurity Beveiligingsplan. Opdrachtnemer dient de blokhaken en alle tekst ertussen te verwijderen en de eigen tekst te plaatsen. De proceseisen zijn direct onder de blokteksten in blauw gekleurde tekst weergegeven en de systeemtechnische eisen in groen gekleurde tekst en betreffen eisen die uitwerking behoeven in de betreffende paragrafen. Het kan voorkomen dat proces of systeemeisen meerdere malen onder verschillende paragrafen terugkomen vanwege raakvlak of overlap. De betreffende proces of systeemtechnische eis hoeft maar één keer uitgewerkt te worden en in dit soort voorkomens kan dan verwezen worden naar de betreffende paragraaf met uitwerking. Het Cybersecurity Beveiligingsplan en het Cybersecurity Dossier dient als synoniem van elkaar gezien te worden. Daar waar in de contract eistekst Cybersecurity Dossier wordt genoemd kan men dit lezen als Cybersecurity Beveiligingsplan.

De Opdrachtnemer dient bij de uitwerking en vastlegging van de contractuele set van cybersecurity eisen in de template Cybersecurity Beveiligingsplan onderscheid te maken naar de generieke en of aannemer specifieke onderdelen en de object specifieke onderdelen. Bij voorkeur dient de template van het Cybersecurity Beveiligingsdossier in meerdere delen ingevuld en onderhouden te worden gedurende de contractlooptijd. Eén voor de generieke en aannemer-specifieke uitwerking van de organisatorische en procesmatige beheersdoelen/controls en één of meerdere object-specifieke delen met de meer systeemtechnische beheersdoelen/controls. Het heeft de voorkeur van Opdrachtgever om bij contracten met in de scope meerdere afzonderlijke objecten voor elk object één object-specifiek deel van het Cybersecurity Beveiligingsdossier op te stellen. Bij opdrachten met beperkte scope en complexiteit kan het handiger zijn om één generiek en één object-specifiek deel van het Cybersecurity Beveiligingsdossier op te stellen. Bij einde van het contract kan dan enkel het object-specifieke deel aan de volgende (onderhouds)aannemer worden meegegeven. Dit onderscheid zal ook bijdragen aan de uniformiteit en herbruikbaarheid van zowel het aannemer-specifieke en het object-specifieke deel van het Cybersecurity Beveiligingsdossier. Afstemming met Opdrachtgever is raadzaam in deze.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber security dossier | Deel | Inhoud | Opslag | Geldigheid |
| Procesdeel | Invulling proces- en managementeisen | Projectarchief | Duur van het contract |
| Objectdeel 1 | Invulling systeemeisen voor object 1 | Areaalinformatie | Levensduur object 1 |
| Objectdeel N | Invulling systeemeisen voor object N | Areaalinformatie | Levensduur object N |

Verder dient bij het opstellen van het Cybersecurity Beveiligingsdossier rekening gehouden te worden met de verantwoordelijkheidsgebieden en verantwoordelijkheden tussen Opdrachtgever en Opdrachtnemer en op de koppelvlakken hiertussen. Onderkend kunnen dan ook worden drie omgevingen met koppelvlakken en wisselwerking:

1. De omgeving van de Opdrachtgever met zijn eigen IV en IA systemen.
Het kan nodig zijn dat Opdrachtnemer toegang moet hebben tot de IV en IA systemen in het verantwoordelijks gebied van Opdrachtgever. De Opdrachtnemer volgt hierbij de beveiligingsuitgangspunten en vigerende policies van Opdrachtgever.
2. Contractueel overeengekomen (areaal) scope en diensten.
De focus en uitwerking van de gevraagde generieke en object-specifieke delen van het Cybersecurity Beveiligingsdossier dienen met name te liggen op de binnen deze scope voorkomende objecten en de hierbinnen aanwezige IV en IA systemen. Vanuit de raakvlakken met de omgeving van Opdrachtgever en Opdrachtnemer kunnen er wel de nodige organisatorische, procesmatige en of technische beheersmaatregelen nodig zijn om de diensten binnen de contract scope mogelijk te maken en de beveiliging te waarborgen.
3. De omgeving van de Opdrachtnemer met zijn eigen IV systemen.
Om de diensten zoals contractueel overeengekomen te kunnen leveren kan het nodig zijn dat Opdrachtnemer voorbereidende of ondersteunende werkzaamheden uitvoert vanuit de eigen kantooromgeving met de eigen IV systemen. De beveiliging van de eigen kantoor en IV systemen van Opdrachtnemer mogen hierbij de beveiliging van de Opdrachtgever niet ondermijnen.

**ISO 27001 of andere certificeringen**
Certificering voor beveiliging van Opdrachtnemer heeft veelal betrekking op de werkomgeving en IV systemen van Opdrachtnemer en dekt niet de areaal scope af zoals contractueel overeengekomen met Opdrachtgever. Certificering zal de Opdrachtnemer wel kunnen helpen om tot een snellere invulling te komen van de gevraagde delen van het cybersecurity beveiligingsdossier maar kan het niet vervangen.

1. Risico’s en eisen uit de Cybersecurity Implementatierichtlijn Objecten
	1. Risico’s

Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval en misbruik van ICT of de Industriële Automatisering (IA). De beheersing van de toegang of het nu fysiek of digitale vorm is, vormt letterlijk en figuurlijk het sleutelbegrip voor het terugdringen van de kwetsbaarheden die benut kunnen worden met gevolgschade en dus risico’s opleveren voor de Infrastructuur in het beheergebied. De eisen uit het contract moeten worden gezien als beheersdoelen/controls die een mogelijk risico probeert af te vangen voor de Infrastructuur. Risico gestuurde aanpak is dan ook mogelijk door middel van de selectie van beheersdoelen/controls die aan het contract worden toegevoegd.

De mitigatie van de volgende top 10 praktijk voorkomens, die risico’s voor het beheerobject kunnen opleveren, worden 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 Opdrachtgever;
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 datanetwerk van Opdrachtgever;
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).
	1. Eisen uit de Cybersecurity Implementatierichtlijn Objecten

Opdrachtnemer geeft invulling aan de cybersecurityeisen zoals contractueel opgelegd. De invulling hiervan wordt gedaan middels de cybersecurity maatregelen uit de bijlage Cybersecurity Implementatierichtlijn Objecten die met het contract is meegegeven. De beheersmaatregelen worden in relatie tot de scope van de opdracht en de geprioriteerde kwetsbaarheden met bijbehorende risico’s door Opdrachtgever samengevoegd met de door [OPDRACHTNEMER] uitgevoerde risicoanalyse en risicoafweging en te treffen beheersmaatregelen nader uitgewerkt in de navolgende hoofdstukken.

|  |  |
| --- | --- |
| 5.1.1VSP01 | De Opdrachtnemer dient de Werkzaamheden met betrekking tot cybersecurity zodanig te verrichten dat het gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen. |
| 5.1.1.1VSP02 | De Opdrachtnemer dient zijn procesbeschrijving (cybersecurity plan) , waarmee invulling wordt gegeven aan de bovenliggende topeis en ten minste aan alle daaraan onderliggende eisen, ter kennis te brengen van de Opdrachtgever. |
| 5.1.1.1VSP55 | De Opdrachtnemer dient het door de Opdrachtgever ter beschikking gestelde template cybersecurity beveiligingsplan of dossier op te bouwen en actueel te houden en op verzoek te leveren aan de opdrachtgever. |

1. Cybersecurity beheersmaatregelen
	1. Objecten en weerstandsniveau

Conform de infraclassificatie van Opdrachtgever dient het volgende cybersecurity weerstandsniveau voor de afzonderlijke objecten aangehouden te worden. Indien het object niet in de lijst infraclassificatie objecten voorkomt dient altijd het cybersecurity weerstandsniveau 1 aangehouden te worden.

Het weerstandsniveau voor de afzonderlijke [objecten] is vastgesteld op [vul weerstandsniveau in per object].

Voor de uitwerking van het generieke Opdrachtnemer specifieke Cybersecurity Beveiligingsplan dient de Opdrachtnemer voor de organisatorische en procesmatige beheersmaatregelen het hoogste cybersecurity weerstandsniveau aan te houden die voorkomt de binnen de contractscope voor de objecten.

Dit Cybersecurity Beveiligingsplan toont aan op welke wijze [OPDRACHTNEMER] invulling geeft aan cybersecurity en voldoet aan de voor dit weerstandsniveau geldende eisen, teneinde gevaar of schade door verstoring, uitval of misbruik van ICT of IA te voorkomen en een goed functioneren te borgen.

Indien de Cybersecurity Implementatie Richtlijn Objecten niet voorziet in maatregelen voor de invulling van de cybersecurityeisen, volgt Opdrachtnemer waar relevant de NEN-ISO/IEC 27002 en IEC 62443.

|  |  |
| --- | --- |
| 5.1.1.1VSP08 | De Opdrachtnemer dient voor alle beheerobjecten die zijn voorzien van ICT en IA de van toepassing verklaarde cybersecuritymaatregelen uit bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces uit te voeren die behoren bij cybersecurity weerstandsniveau 1, tenzij er voor een object een ander cybersecurity weerstandsniveau is aangegeven in bijlage A “Informatie Areaal” bij de Vraagspecificatie.. |
| 5.1.1.1VSP09 | Indien bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces niet voorziet in cybersecuritymaatregelen voor de invulling van de cybersecurity eisen, dan dient de Opdrachtnemer de NEN-ISO/IEC 27002 (Code voor Informatiebeveiliging) en/of delen van de IEC 62443 standaards (Industrial Automation and Control Systems (IACS) Security) te volgen. |
| 14.1.1VSP10 | De Opdrachtnemer dient met betrekking tot het beheren en onderhouden van cybersecuritymaatregelen conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 5.1.1.1VSE02 | De ICT en IA van het beheerobject dient daar waar direct of indirect verwezen wordt naar de specifieke implementatie-richtlijnen uit de [Cybersecurity Implementatierichtlijn Objecten] te voldoen aan het Cybersecurity weerstandsniveau [NTB]. |

* 1. Scope

De scope van dit Cybersecurity Beveiligingsplan / Beveiligingsdossier bepaalt voor welke delen van het object, installatie of dienst(verlening) dit geldt.

* + 1. Binnen scope

De volgende zaken vallen binnen scope van dit Cybersecurity Beveiligingsdossier:

* [BESCHRIJF BULLETSGEWIJS DE SCOPE]
	+ 1. Buiten scope

De volgende zaken vallen buiten scope van dit Cybersecurity Beveiligingsdossier:

* [BESCHRIJF BULLETSGEWIJS WELKE ZAKEN BUITEN SCOPE GESTELD ZIJN, INDIEN VAN TOEPASSING]
	1. Comply or explain

[ motiveer in deze paragraaf welke Cybersecurity eisen uit het contract/overeenkomst niet of afwijkend worden ingevuld in relatie tot de scope van het Cybersecurity BeveiligingsDOSSIER, zoals beschreven in paragraaf 2.1 voor het betreffende object, installatie of dienst(verlening).]

|  |  |
| --- | --- |
| 5.1.1.1VSP11 | Indien de Opdrachtnemer tijdelijk niet aan cybersecurityeisen dreigt te voldoen, dan dient de Opdrachtnemer dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem en dient de Opdrachtnemer deze afwijkingenrapportage ter kennis te brengen van de Opdrachtgever en op te nemen in het cybersecurity dossier. |

* 1. Risico’s

[ beschrijf 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 S. De Opdrachtnemer dient voor deze installatie, object of dienst(verlening) minimaal de door Opdrachtgever in paragraaf 1.1 aangegeven KWETSBAArHEDEN en gerelateerde risico’s te mitigeren.

Indien de door Opdrachtgever aangegeven Kwetsbaarheden en gerelateerde risico’s niet van toepassing zijn voor het betreffende object, installatie of dienst(verlening), dan dient dit gemotiveerd te worden bij paragraaf 2.2 waar de ‘comply or explain’ regel geldt.]

|  |  |
| --- | --- |
| 5.1.1.1VSP55 | De Opdrachtnemer dient het door de Opdrachtgever ter beschikking gestelde cybersecurity dossier op te bouwen en actueel te houden en op verzoek te leveren aan de Opdrachtgever. |
| 14.1.1.1VSP04 | De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever. |
| 5.1.1VSE01 | De ICT en IA van het beheerobject dient zodanig te zijn ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen. |

* 1. Beheersmaatregelen

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

* + 1. Cybersecurity aanpak, standaarden en beheersmaatregelen

[BESCHRIJF WELKE PROCES EN AANPAK GEVOLGD GAAT WORDEN EN OP WIJZE INVULLING IS GEGEVEN AAN DE CYBERSECURITY EISENSET, WAAR AANVULLEND GEBRUIK IS GEMAAKT VAN NEN-ISO/IEC 27002 EN/OF IEC 62443, ALSOOK HOE DE KENNIS OMTRENT DEZE NORMEN IS GEBORGD BINNEN DE ORGANISATIE.]

|  |  |
| --- | --- |
| 5.1.1.1VSP09 | Indien bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces niet voorziet in cybersecuritymaatregelen voor de invulling van de cybersecurity eisen, dan dient de Opdrachtnemer de NEN-ISO/IEC 27002 (Code voor Informatiebeveiliging) en/of delen van de IEC 62443 standaards (Industrial Automation and Control Systems (IACS) Security) te volgen. |

* + 1. Belegging verantwoordelijkheden

Bij [OPDRACHTNEMER] is de verantwoordelijkheid voor Cybersecurity belegd bij [afdeling/onderdeel] en is [NAAM PERSOON] voor Opdrachtgever het eerste aanspreekpunt voor Cybersecurity aangelegenheden. Bij afwezigheid zijn de vervangers bekend.

|  |  |
| --- | --- |
| 18.2.1.1VSP62 | De Opdrachtnemer dient in zijn projectmanagementplan ten minste de volgende onderwerpen specifiek voor de opdracht te beschrijven:9. de projectorganisatie waarin ten minste de leidinggevende functies en sleutelfuncties zijn weergegeven met hun taken, verantwoordelijkheden en bevoegdheden; |
| 6.1.1VSP05 | De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de Werkzaamheden met betrekking tot cybersecurity. |

* + 1. Borging Cybersecurity

[BESCHRIJF HOE het beheer en onderhoud van de Cybersecurity beheersmaatregelen ZIJN geborgd in DE processen VAN OPDRACHTGEVER]

|  |  |
| --- | --- |
| 18.2.1.1VSP63 | De Opdrachtnemer dient in zijn projectmanagementplan ten minste de volgende onderwerpen specifiek voor de opdracht te beschrijven:5. de processen, gebruikmakende van procesbeschrijvingen conform het(de) gecertificeerde kwaliteitsmanagementsysteem(en), waarbij ten minste invulling wordt gegeven aan de in de Overeenkomst gestelde proceseisen en waarmee de Opdrachtnemer aantoont dat deze processen het vermogen hebben om het beoogde resultaat te bereiken; |
| 14.1.1VSP10 | De Opdrachtnemer dient met betrekking tot het beheren en onderhouden van cybersecuritymaatregelen conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 14.1.1VSE32 | ICT en IA van het beheerobject dient voor beheer en onderhoud ingericht te zijn conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.1.1VSE33 | Bij inzet van (web)applicaties voor beheer of onderhoud van ICT en IA van het beheerobject dient de beveiliging van de in te zetten (web)applicaties ingericht te zijn conform de [ICT-Beveiligingsrichtlijnen Webapplicaties] van het Nationaal Cybersecurity Centrum. |
| 14.2.5VSE37 | De cybersecurity eisen zijn onverkort van toepassing voor de inrichting en onderhoud van eventuele (permanente) Ontwikkel-, Test-, Acceptatie- en Leeromgevingen voor de ICT en IA van het beheerobject, inclusief de vereisten uit paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Onderaannemers

[beschrijf 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.]

|  |  |
| --- | --- |
| 7.2.118.2.2VSP64 | De Opdrachtnemer vereist dat zijn (zelfstandige) hulppersonen de cybersecurity eisen en maatregelen toepassen in overeenstemming met de vastgestelde beleidsregels en procedures. |
| 14.2.6.1VSP61 | Indien de Opdrachtnemer Werkzaamheden door zelfstandige hulppersonen wil laten verrichten, dan dient de Opdrachtnemer een quickscan conform de handleiding "Quickscan nationale veiligheid bij inkoop en aanbesteden" uit te voeren en het resultaat ter kennis te brengen van de Opdrachtgever. |
| 7.1.1VSP27 | De Opdrachtnemer dient de Werkzaamheden aan:1. ontwerp- en constructietekeningen en constructieberekeningen en/of;2. beveiligings- en veiligheidsdocumentatie en -instructies van:a. kunstwerken;b. bediengebouwen en -ruimten;d. ICT en IA;e. Kabels en leidingen;dan wel de Werkzaamheden:3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten;4. aan ICT en IA zelf;5. aan kabels en leidingendoor (zelfstandige) hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en 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 start van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende (zelfstandige) hulppersoon. |

* + 1. Beheer bedrijfsmiddelen en CMDB

[beschrijf conform CYBERSECURITY Richtlijn 16 “REGISTRATIE CI ITEMS IN EEN CONFIGURATION MANAGEMENT DATABASE” 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.]

|  |  |
| --- | --- |
| 8.1.1VSP56 | De Opdrachtnemer dient alle configurations items (CI's) van de ICT en IA conform de bijlage CSR 16 "Registratie assets in een configuratiemanagement database (CMDB)" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te registreren in een door de Opdrachtgever beschikbaar gesteld Excel format en te leveren aan de Opdrachtgever. |
| 13.1.3VSP39 | De Opdrachtnemer dient met betrekking tot het datanetwerk, conform paragraaf 2.4.1 "Netwerkkoppelingen" en conform de bijlage CSR 3 "Architectuur objectnetwerk" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |

* + 1. Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever

[beschrijf op welke wijze een aanvaardbaar gebruik WORDT BEWERKSTELLIGD van door Opdrachtgever eventueel beschikbaar gestelde toegangsmiddelen (pasjes, tokens, e.d.) en een HOE EEN sluitende administratie WORDT bijhoudEN aan de kant van Opdrachtnemer.]

|  |  |
| --- | --- |
| 9.1.1VSP28 | De Opdrachtnemer dient voor de toegang tot beheerobjecten de bijlage CSR 2 "Personele Toegang" van bijlage V "Cybersecurity Implementatierichtlijn objecten" bij deze Vraagspecificatie Proces, te volgen. |
| 7.1.2VSP29 | De Opdrachtnemer draagt er zorg voor dat zijn (zelfstandige) hulppersonen de huis- en gedragsregels zoals vastgelegd in de bijlage CSR 17 "Beveiligingshuisregels" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, kennen en naleven. |
| 9.2.1VSP32 | "De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van:1. de door de Opdrachtnemer aan de (zelfstandige) hulppersonen verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen;2. de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten." |
| 8.1.3VSP37 | De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot beheerobjecten, 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. |
| 8.1.4VSP38 | De Opdrachtnemer dient alle door de Opdrachtgever ter beschikking gestelde bedrijfsmiddelen nadat ze niet meer van dienst zijn geworden doch uiterlijk bij beëindiging van de Overeenkomst terug te geven. |

* + 1. Classificatie en beveiliging informatie

[beschrijf HOE conform CYBERSECURITY Richtlijn 1 “OMGAAN MET VERTROUWELIJKE INFORMATIE EN DOCUMENTEN” WORDT omGEgaan met vertrouwelijke informatie en documenten, EN op welke wijze de beveiliging wordt bewerkstelligd van door Opdrachtgever aangegeven vertrouwelijke documenten, zoals ontwerp, constructietekeningen en datanetwerkschema’s.]

|  |  |
| --- | --- |
| 15.1.1.318.1.4VSP19 | Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt, dan dient de Opdrachtnemer een verwerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon “verwerkersovereenkomst” dat de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt. |
| 8.2.1VSP21 | De Opdrachtnemer dient voor de beveiliging van informatie van de Opdrachtgever en van Documenten, de door de Opdrachtgever aangegeven document-classificatie en bijbehorende beveiligingsmaatregelen conform de bijlage CSR 1 “Omgaan met vertrouwelijke informatie en documenten” van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, aan te houden. |
| 8.3.2.118.1.3VSP22 | De Opdrachtnemer dient het deel van zijn informatievoorziening, dat benodigd is voor de door de Opdrachtgever gevraagde Documenten en dat benodigd is bij de verwerking van de door de Opdrachtgever ter beschikking gestelde informatie, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging. |
| 8.3.2.2VSP24 | De Opdrachtnemer dient uiterlijk bij beëindiging van de Overeenkomst alle Documenten en door de Opdrachtgever ter beschikking gestelde informatie die kwetsbaarheden kunnen veroorzaken voor de Opdrachtgever en die niet eerder zijn overgedragen alsnog over te dragen aan de Opdrachtgever. Datgene wat is overgedragen en wat niet wordt of niet kan worden overgedragen, dient te worden gewist en/of vernietigd in de informatievoorziening van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst. |
| 8.3.2.2VSP25 | Indien de Opdrachtnemer ICT- en IA-componenten en/of de daarop aanwezige informatie verwijdert, hergebruikt en/of vernietigt, dan dient hij conform de bijlage CSR 23 "Verwijdering en vernietiging van informatie en apparatuur" van bijlage V "Cybersecurity Implementatierichtlijn objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 8.1.4VSP38 | De Opdrachtnemer dient alle door de Opdrachtgever ter beschikking gestelde bedrijfsmiddelen nadat ze niet meer van dienst zijn geworden doch uiterlijk bij beëindiging van de Overeenkomst terug te geven. |

* + 1. Bewustwording, scholing en VOG

[beschrijf 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.]

|  |  |
| --- | --- |
| 7.1.1VSP27 | De Opdrachtnemer dient de Werkzaamheden aan:1. ontwerp- en constructietekeningen en constructieberekeningen en/of;2. beveiligings- en veiligheidsdocumentatie en -instructies van:a. kunstwerken;b. bediengebouwen en -ruimten;d. ICT en IA;e. Kabels en leidingen;dan wel de Werkzaamheden:3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten;4. aan ICT en IA zelf;5. aan kabels en leidingendoor (zelfstandige) hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en 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 start van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende (zelfstandige) hulppersoon. |
| 7.1.2VSP29 | De Opdrachtnemer draagt er zorg voor dat zijn (zelfstandige) hulppersonen de huis- en gedragsregels zoals vastgelegd in de bijlage CSR 17 "Beveiligingshuisregels" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, kennen en naleven. |
| 7.2.17.2.2VSP26 | De Opdrachtnemer dient met betrekking tot bewustwording en training van (zelfstandige) hulppersonen, voor zover relevant voor hun functie, conform paragraaf 2.7 "Maatregelen Bewustwording en Training" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |

* + 1. Fysieke (toegangs)beveiliging tot object, technische- en bedienruimten

[beschrijf 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.

|  |  |
| --- | --- |
| 9.1.1VSP35 | De Opdrachtnemer dient met betrekking tot de logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten conform paragraaf 2.2 "Maatregelen Logische Toegang" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 9.1.1VSP28 | De Opdrachtnemer dient voor de toegang tot beheerobjecten de bijlage CSR 2 "Personele Toegang" van bijlage V "Cybersecurity Implementatierichtlijn objecten" bij deze Vraagspecificatie Proces, te volgen. |
| 9.2.1VSP32 | De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van:1.    de door de Opdrachtnemer aan de (zelfstandige) hulppersonen verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen;2.    de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten. |
| 11.1.1VSP33 | De (beheer)processen voor de fysieke beveiliging van het terrein en gebouwen hierbinnen dienen conform paragraaf 2.1.2 “Fysieke beveiliging terrein en gebouwen” en CSR 24 “Fysieke beveiligingsmaatregelen” ingevuld te worden.  |
| 11.1.2VSP34 | De Opdrachtnemer dient met betrekking tot fysieke toegangsbeveiliging van de ICT en IA gerelateerde ruimten (waaronder bedien- en technische ruimten) binnen beheerobjecten, conform paragraaf 2.1.1 "Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 11.1.1VSE 10 | De fysieke beveiliging van het terrein en gebouwen hierbinnen behorende bij het beheerobject dienen conform paragraaf 2.1.2 “Fysieke beveiliging terrein en gebouwen” en CSR 24 “Fysieke beveiligingsmaatregelen” ingevuld te worden. |
| 11.1.1.1VSE 11 | De fysieke toegangsbeveiliging van ICT en IA gerelateerde ruimten (waaronder Bedienruimte en Technische Ruimten) van het beheerobject dient ingericht te zijn conform paragraaf 2.1 "Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 11.1.411.2.6VSE 13 | De ICT en IA van het beheerobject dient, indien geplaatst buiten beveiligde gebouwen en ruimten, op basis van een risico analyse en afweging geplaatst te zijn in afsluitbare kasten of ruimten, die bij fysieke opening een alarmmelding genereren, die opgevolgd wordt, evenals bij ongeautoriseerde logische toegang tot het datanetwerk in de kast of ruimte. |

* + 1. Logische toegangsbeveiliging tot ICT en IA-systemen

[beschrijf 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.]

|  |  |
| --- | --- |
| 9.1.1VSP35 | De Opdrachtnemer dient met betrekking tot de logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten conform paragraaf 2.2 "Maatregelen Logische Toegang" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 9.1.1VSP28 | De Opdrachtnemer dient voor de toegang tot beheerobjecten de bijlage CSR 2 "Personele Toegang" van bijlage V "Cybersecurity Implementatierichtlijn objecten" bij deze Vraagspecificatie Proces, te volgen. |
| 9.2.1VSP32 | De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van:1.    de door de Opdrachtnemer aan de (zelfstandige) hulppersonen verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen;2.    de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten. |
| 9.1.1VSE 5 | Voor de ICT en IA van beheerobject dient voor de identificatie, authenticatie en autorisatie oplossing maatregelen te implementeren conform paragraaf 2.2 "Maatregelen logische toegang" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Wachtwoordrichtlijn

[beschrijf op welke wijze invulling wordt gegeven aan de door Opdrachtgever beschikbaar gestelde CYBERSECURITY Richtlijn 7 “WACHTWOORDEN”. motiveer afwijkingen en controleer periodiek de naleving ERVAN door personeel.]

|  |  |
| --- | --- |
| 9.3.1VSP36 | De Opdrachtnemer dient voor een zorgvuldige omgang met de aan hem toevertrouwde accounts en bijbehorende wachtwoorden, conform de bijlage CSR 7 “Wachtwoorden" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, te handelen. |
| 9.3.1VSE 6 | Voor de ICT en IA van het beheerobject dient voor eisen en functionaliteit ten aanzien van wachtwoorden maatregelen te implementeren conform bijlage CSR 7 "Wachtwoorden" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Back-up en recovery proces

[beschrijf 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.

De Opdrachtnemer test jaarlijks het recovery proces en beschrijft de resultaten ook in het hoofdstuk 7 ‘Evaluatie en actualisatie beheersmaatregelen’.]

|  |  |
| --- | --- |
| 12.3.1VSP58 | De Opdrachtnemer dient een protocol voor back-up en recovery , conform paragraaf 2.10 “Maatregelen Back-ups” en conform de bijlage CSR 18 "Back-up en Recovery" van de bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, op te stellen en te leveren aan de Opdrachtgever. |
| 12.3.1VSE 19 | De integriteit en beschikbaarheid van de ICT en IA van het beheerobject dient geborgd te zijn doormiddel van back-ups conform paragraaf 2.10 "Maatregelen back-ups" en bijlage CSR 18 "Back-up en recovery" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Documentatie bediening en beheer

[GEEF EEN OVERZICHT VAN DOCUMENTEN DIE ZIJN OPGESTELD VOOR DE BEDIENING, HET BEHEER, HET ONDERHOUD EN DE TECHNISCHE ONDERSTEUNING VAN ICT EN IA.

BESCHRIJF HOE DEZE DOCUMENTEN WORDEN ONDERHOUDEN.]

|  |  |
| --- | --- |
| OW310 | De Opdrachtnemer dient van de gegenereerde oplossingen voor (de onderdelen van) het Werk ten minste het volgende vast te leggen:4. de gemaakte ontwerpkeuzes inclusief onderbouwing (waaronder de analyses);6. de aspecten van integrale veiligheid tijdens realisatie, gebruik, beheer, onderhoud en sloop;10. de wijze van uitvoering en/of integratie; 11. de wijze van onderhouden; 12. indien van toepassing: de wijze van bediening. |

* + 1. Beveiliging documentatie

[beschrijf op welke wijze de bedien- , beheer en technische documentatie beschermd wordt tegen verlies en ongeautoriseerde kennisname of wijziging.]

|  |  |
| --- | --- |
| 8.3.2.118.1.3VSP22 | De Opdrachtnemer dient het deel van zijn informatievoorziening, dat benodigd is voor de door de Opdrachtgever gevraagde Documenten en dat benodigd is bij de verwerking van de door de Opdrachtgever ter beschikking gestelde informatie, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging. |
| 8.3.2.2VSP24 | De Opdrachtnemer dient uiterlijk bij beëindiging van de Overeenkomst alle Documenten en door de Opdrachtgever ter beschikking gestelde informatie die kwetsbaarheden kunnen veroorzaken voor de Opdrachtgever en die niet eerder zijn overgedragen alsnog over te dragen aan de Opdrachtgever. Datgene wat is overgedragen en wat niet wordt of niet kan worden overgedragen, dient te worden gewist en/of vernietigd in de informatievoorziening van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst. |
| 10.1.1VSP41 | Indien de Opdrachtnemer cryptografie inzet ter bescherming van vertrouwelijkheid, authenticiteit en/of integriteit van Documenten en informatie, dan dient hij, conform paragraaf 2.4.2 "Cryptografie" van bijlage V "Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |

* + 1. Ontwikkeling, onderhoud en wijzigingsproces

[beschrijf hier het proces dat gevolgd wordt voor ontwikkeling, onderhoud en het doorvoeren van (functionele) wijzigingen aan ICT en IA conform de eisen uit de overeenkomst en de Cybersecurity Implementatie Richtlijn Objecten. In voorkomende gevallen dienen security gerelateerde wijzigingen gerapporteerd en specifiek in hoofdstuk 7 te worden uitgeschreven.]

|  |  |
| --- | --- |
| 7.2.118.2.1.1 VSP64 | De Opdrachtnemer vereist dat zijn (zelfstandige) hulppersonen de cybersecurity eisen en maatregelen toepassen in overeenstemming met de vastgestelde beleidsregels en procedures. |
| 6.2.1VSP42 | De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en IA van de Opdrachtgever de bijlage CSR 4 "Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, aan te houden voor bescherming tegen malware. |
| 6.2.1.2VSP43 | De Opdrachtnemer dient maximale hardening toe te passen voor zijn (rand)apparatuur en (delen van) zijn eigen datanetwerkinfrastructuur die ten behoeve van de Werkzaamheden gekoppeld zijn aan de datanetwerkinfrastructuur van de Opdrachtgever. |
| 6.2.1.2VSE04 | Maximale hardening conform de maatregelen uit paragraaf 2.5.2 “Hardening” en bijlage CSR9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten] dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject. |
| 12.1.2VSP49 | De Opdrachtnemer dient met betrekking tot het doorvoeren van Wijzigingen aan bestaande ICT en IA, conform paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen |
| 14.2.718.2.3.1VSP50 | De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever. |
| 12.1.4VSE 15 | De Ontwikkel-, Test-, Acceptatie-, Productie-, en Leeromgeving van het beheerobject dient gescheiden te zijn om het risico van onbevoegde toegang tot of veranderingen aan de productie omgeving te verlagen. |
| 13.1.3VSE29 | Voor de ICT en IA van het beheerobject dient segmentering van dataverkeersstromen toegepast te zijn voor Ontwikkel-, Test-, Acceptatie-, Productie-, Leer- en Beheeromgeving. |
| 14.2.5VSE 37 | De cybersecurity eisen zijn onverkort van toepassing voor de inrichting en onderhoud van eventuele (permanente) Ontwikkel-, Test-, Acceptatie- en Leeromgevingen voor de ICT en IA van het beheerobject inclusief de vereisten uit paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.2.7VSE 38 | De ICT en IA van het beheerobject dienen als integraal onderdeel van de FAT, SAT en SIT getest te zijn op technische naleving van beveiligingseisen en het aantoonbaar maken van de werking van de security functies en maatregelen. |

* + 1. Beveiliging tegen malware, hardening en patching

[beschrijf 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).]

|  |  |
| --- | --- |
| 12.2.1VSP54 | Indien ICT en IA niet beschermd worden door antimalware oplossingen, dan dient de Opdrachtnemer ten minste jaarlijks, conform de bijlage CSR 11 "Malware scanning en opschoning middels een usb" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te scannen op malware en aangetroffen malware te verwijderen. |
| 12.6.1VSP51 | De Opdrachtnemer dient met betrekking tot het patchen van de ICT en IA, conform paragraaf 2.5 “Maatregelen bescherming tegen kwetsbaarheden” en conform de bijlage CSR 8 “Patch management" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| VSP52 | Indien de Opdrachtnemer meent geen gebruik te maken van de mogelijkheid om te patchen, dan dient hij een gemotiveerd voorstel  ter kennis te brengen van de Opdrachtgever. |
| 12.1.4VSE16 | De ICT en IA van het beheerobject dient beschermd te zijn tegen malware conform de maatregelen uit paragraaf 2.5.1 "Anti-malware" en bijlage CSR 11 “Malware scanning en opschoning middels een USB“ van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 12.2.1VSE17 | De ICT en IA van het beheerobject dient gehardend te zijn conform de maatregelen uit paragraaf 2.5.2 "Hardening" en bijlage CSR 9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 12.2.1VSE18 | De ICT en IA van het beheerobject dient gepatcht te zijn conform de maatregelen uit paragraaf 2.5.3 “Patching” en bijlage CSR 8 “Patch management” van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Patch proces en kritieke Patches

[beschrijf 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.]

|  |  |
| --- | --- |
| 5.1.1.1VSP11 | Indien de Opdrachtnemer tijdelijk niet aan cybersecurityeisen dreigt te voldoen, dan dient de Opdrachtnemer dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem en dient de Opdrachtnemer deze afwijkingenrapportage  ter kennis te brengen van de Opdrachtgever en op te nemen in het Cybersecurity Dossier. |
| 12.6.1VSP51 | De Opdrachtnemer dient met betrekking tot het patchen van de ICT en IA, conform paragraaf 2.5 “Maatregelen bescherming tegen kwetsbaarheden” en conform de bijlage CSR 8 “Patch management" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 12.6.1.1VSP52 | Indien de Opdrachtnemer meent geen gebruik te maken van de mogelijkheid om te patchen, dan dient hij een gemotiveerd voorstel  ter kennis te brengen van de Opdrachtgever. |
| 12.6.1.1VSP53 | Indien de Opdrachtgever melding maakt van een kritieke of niet kritieke patch dan dient de Opdrachtnemer daarvoor een implementatieadvies  ter kennis te brengen van de Opdrachtgever. Daarbij gelden de volgende doorlooptijden: 1.    voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;2.    voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever. De Opdrachtnemer dient de patch, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren. |
| 12.2.1VSE18 | De ICT en IA van het beheerobject dient gepatcht te zijn conform de maatregelen uit paragraaf 2.5.3 “Patching” en bijlage CSR 8 “Patch management” van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Koppeling van apparatuur

[beschrijf conform CYBERSECURITY Richtlijn 4 “hET veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van ” 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.]

|  |  |
| --- | --- |
| 6.2.1VSP42 | De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en IA van de Opdrachtgever de bijlage CSR 4 "Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, aan te houden voor bescherming tegen malware. |
| 6.2.1.2VSP43 | De Opdrachtnemer dient maximale hardening toe te passen voor zijn (rand)apparatuur en (delen van) zijn eigen datanetwerkinfrastructuur die ten behoeve van de Werkzaamheden gekoppeld zijn aan de datanetwerkinfrastructuur van de Opdrachtgever. |
| 5.1.1.1VSP45 | Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) (pen)testen van (delen van) zijn datanetwerk. |

|  |  |
| --- | --- |
| 5.1.1.1VSP46 | Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) monitoren van (delen van) zijn datanetwerk. |

|  |  |
| --- | --- |
| 6.2.1.2VSE04 | Maximale hardening conform de maatregelen uit paragraaf 2.5.2 “Hardening” en bijlage CSR9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten] dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject. |

* + 1. Logging en monitoring

[beschrijf op welke wijze logging en monitoring wordt vormgegeven qua proces en voorzieningen in aansluiting op de eisen uit de Cybersecurity Implementatierichtlijn Objecten.]

|  |  |
| --- | --- |
| 12.4.1.3VSP44 | De Opdrachtnemer dient met betrekking tot het kunnen koppelen aan het SOC van de Opdrachtgever, conform paragraaf 2.6 "Maatregelen logging en monitoring" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 12.4.1VSE20 | De ICT en IA van het beheerobject dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vast te leggen in logbestanden conform paragraaf 2.6 “Maatregelen logging en monitoring” en bijlage CSR 10 "Logging" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 12.4.1VSE21 | Voor de ICT en IA van het beheerobject dient een (centrale) syslog server ingericht te zijn die syslog events verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen door een Security Information & Event Management (SIEM) systeem en/of een Security Operations Centre (SOC) conform paragraaf 2.6 “Maatregelen logging en monitoring” en bijlage CSR 10 “Logging” van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 12.4.1VSE22 | De ICT en IA van het beheerobject dient technisch te zijn voorbereid op monitoring middels detectievoorzieningen van het Security Operations Centre (SOC) van Opdrachtgever conform paragraaf 2.6 "Maatregelen logging en monitoring" van de [Cybersecurity Implementatie Richtlijn Objecten]. |
| 12.4.1.3VSE23 | Het objectdatanetwerk van het beheerobject dient uitgevoerd te zijn met analysepoorten door poorten in het lokale objectdatanetwerk tot analyse poort te configureren. |

* + 1. Bewijsmateriaal verzamelen en bewaren

[BESCHRIJF OP WELKE WIJZE OPDRACHTNEMER IN VOORKOMENDE GEVALLEN DE OPDRACHTGEVER MEDEWERKING VERLEENT VOOR HET VERZAMELEN, BEWAREN EN BESCHIKBAAR STELLEN VAN CYBERSECURITY BEWIJSMATERIAAL.]

|  |  |
| --- | --- |
| 16.1.7VSP17 | De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal. |

* + 1. Datanetwerkinrichting en datanetwerkkoppelingen

[geef 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.]

|  |  |
| --- | --- |
| 5.1.1.1VSP45 | Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) (pen)testen van (delen van) zijn datanetwerk. |
| 5.1.1.1VSP46 | Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risico gestuurd (laten) monitoren van (delen van) zijn datanetwerk. |
| 12.4.1.3VSP44 | De Opdrachtnemer dient met betrekking tot het kunnen koppelen aan het SOC van de Opdrachtgever, conform paragraaf 2.6 "Maatregelen logging en monitoring" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 13.1.1VSP40 | De Opdrachtnemer dient met betrekking tot datanetwerkkoppelingen, conform paragraaf 2.4.1 "Netwerkkoppelingen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 13.1.3VSP39 | De Opdrachtnemer dient met betrekking tot het datanetwerk, conform paragraaf 2.4.1 "Netwerkkoppelingen" en conform de bijlage CSR 3 "Architectuur objectnetwerk" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 13.1.1VSE24 | De datanetwerkkoppelingen van het beheerobject dienen uitgevoerd te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 13.1.1VSE26 | Het aantal ICT en IA datanetwerkkoppelingen van het beheerobject met andere externe datanetwerken dient geminimaliseerd te zijn. |
| 13.1.3VSE28 | Voor de ICT en IA van het beheerobject dient gebruik te zijn gemaakt van een gecompartimenteerde datanetwerk dat van de kantoorautomatisering is gescheiden. De scheiding kan fysiek of logisch zijn. |
| 13.1.3VSE30 | De ICT en IA datanetwerken van het beheerobject dienen ingericht te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Remote Access

[beschrijf 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.

in het geval van remote acces via de RAS oplossing dient opdrachtnemer een sluitende administratie erop na te houden over de door Opdrachtgever verstrekte tokens of andere middelen voor toegang. Alle bedrijfsmiddelen van Opdrachtgever moeten bij einde overeenkomst worden ingeleverd.]

|  |  |
| --- | --- |
| 9.4.2.2VSP30 | Indien de Opdrachtnemer toegang tot ICT en IA op afstand (remote access) wenst, dan dient de Opdrachtnemer deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van de Opdrachtgever te laten verlopen. |
| 9.4.2.2VSP31 | Indien de Opdrachtnemer toegang tot ICT en IA op afstand (remote access) wenst, dan 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. |
| 13.1.1VSP40 | De Opdrachtnemer dient met betrekking tot datanetwerkkoppelingen, conform paragraaf 2.4.1 "Netwerkkoppelingen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 13.1.3VSP39 | De Opdrachtnemer dient met betrekking tot het datanetwerk, conform paragraaf 2.4.1 "Netwerkkoppelingen" en conform de bijlage CSR 3 "Architectuur objectnetwerk" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 13.1.1VSE24 | De datanetwerkkoppelingen van het beheerobject dienen uitgevoerd te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 13.1.1VSE25 | Alle datanetwerkverbindingen van het beheerobject dienen strikt en uitsluitend te verlopen via centrale beveiligde voorzieningen.Directe vaste of draadloze datanetwerkverbindingen met andere datanetwerken dan die van Opdrachtgever zijn strikt verboden. |

* + 1. Gebruik veilige communicatieprotocollen en draadloze netwerken

[beschrijf 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 beheerobject 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.]

|  |  |
| --- | --- |
| 10.1.1VSP41 | Indien de Opdrachtnemer cryptografie inzet ter bescherming van vertrouwelijkheid, authenticiteit en/of integriteit van informatie, dan dient hij, conform paragraaf 2.4.2 "Cryptografie" van bijlage V "Cybersecurity Implementatierichtlijn Objecten” bij de Vraagspecificatie, cybersecuritymaatregelen te treffen. |
| 10.1.1VSE07 | Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling ter bescherming van de vertrouwelijkheid, authenticiteit en/of integriteit maatregelen getroffen te worden conform paragraaf 2.4.2 "Cryptografie" van de [Cybersecurity Implementatierichtlijn Objecten].  |
| 10.1.1VSE08 | Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling alleen gekozen te worden voor de versleuteling, de onderliggende algoritmes en instellingen met uitsluitend de duiding “goed”, zoals aangegeven in het NCSC document [Richtlijnen voor Transport Layer Security]. |
| 10.1.1VSE09 | Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling gebruik gemaakt te worden van: - PKI-Overheid certificaten voor communicatie met externe netwerken- Organisatie eigen interne PKI certificaten voor communicatie met interne netwerken |
| 13.1.1VSE26 | Het aantal ICT en IA datanetwerkkoppelingen van het beheerobject met andere externe datanetwerken dient geminimaliseerd te zijn. |
| 13.1.2.3VSE27 | Draadloze netwerken van het beheerobject zijn ingericht conform paragraaf 2.4.2 "Cryptografie” en bijlage CSR 5 "Draadloze netwerken" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.1.1VSE34 | Voor het beheerobject dient de toepassing van IoT gebaseerd te zijn op de uitkomsten van een risico en privacy assessment en voorzien te zijn van relevante mitigerende maatregelen conform bijlage CSR 6 "IoT" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Applicaties ontwikkeling en onderhoud

[Beschrijf, voor (web)applicaties voor bediening en beheer (op afstand) van het beheerobject, hoe de beveiliging van de (web)applicatie is vormgegeven en in hoeverre deze voldoet aan de Security Eisen van Opdrachtgever.]

|  |  |
| --- | --- |
| 14.2.5VSP07 | Indien de Opdrachtnemer een test- en ontwikkelomgeving dient in te richten, dan dient hij daarbij de eisen ten aanzien van cybersecurity toe te passen. |
| 14.2.1.1VSP47 | De Opdrachtnemer dient voor het ontwikkelen en/of het onderhouden van software de gangbare principes en de voorgeschreven maatregelen uit het document "Grip op Secure Software Development (SSD) Beveiligingseisen voor (web)applicaties" van het Centrum Informatiebeveiliging en Privacybescherming (CIP) te volgen. |
| 14.2.718.2.3.1VSP50 | De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever. |
| 14.1.1VSE31 | ICT en IA van het beheerobject dient voorzien te zijn van invoer en uitvoer validatie controles om corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken. |
| 14.1.1VSE32 | ICT en IA van het beheerobject dient voor beheer en onderhoud ingericht te zijn conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.1.1VSE33 | Bij inzet van (web)applicaties voor beheer of onderhoud van ICT en IA van het beheerobject dient de beveiliging van de in te zetten (web)applicaties ingericht te zijn conform de [ICT-Beveiligingsrichtlijnen Webapplicaties] van het Nationaal Cybersecurity Centrum. |
| 14.1.1VSE34 | Voor het beheerobject dient de toepassing van IoT gebaseerd te zijn op de uitkomsten van een risico en privacy assessment en voorzien te zijn van relevante mitigerende maatregelen conform bijlage CSR 6 "IoT" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.1.1VSE35 | Gevirtualiseerde ICT en IA van het beheerobject dient ingericht te zijn conform bijlage CSR 22 “Virtualisatie” van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.2.1.1VSE36 | De software van ICT en IA van het beheerobject dient ontwikkeld en beheerd te zijn volgens gangbare principes en de voorgeschreven maatregelen conform Secure Software Development (SSD) van het Centrum voor Informatiebeveiliging en Privacy (CIP). |
| 14.2.5VSE37 | De cybersecurity eisen zijn onverkort van toepassing voor de inrichting en onderhoud van eventuele (permanente) Ontwikkel-, Test-, Acceptatie- en Leeromgevingen voor de ICT en IA van het beheerobject, inclusief de vereisten uit paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 14.2.7VSE38 | De ICT en IA van het beheerobject dienen als integraal onderdeel van de FAT, SAT en SIT getest te zijn op technische naleving van beveiligingseisen en het aantoonbaar maken van de werking van de security functies en maatregelen. |

* + 1. Continuïteit en herstel dienstverlening

[beschrijf 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.]

|  |  |
| --- | --- |
| 17.2.2VSP59 | De Opdrachtnemer dient een continuïteitsplan voor energievoorziening op te stellen conform de bijlage CSR 12 "Continuïteitsplan voor energievoorziening" van bijlage [#?#] “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces en te leveren aan de Opdrachtgever. |
| 17.2.2VSP60 | De Opdrachtnemer dient de continuïteitsplannen voor energievoorziening die ter beschikking zijn gesteld in bijlage A “Informatie Areaal” bij de Vraagspecificatie ten minste jaarlijks uit te voeren, actueel te houden en te leveren aan de opdrachtgever. |
| 5.1.1.1VSP57 | De Opdrachtnemer dient conform bijlage CSR 15 "Recoveryplan" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, een recoveryplan op te stellen, waarmee tevens een succesvolle cyberaanval op de ICT en IA (assume breach) wordt afgedekt en te leveren aan de Opdrachtgever. |
| 12.3.1VSP58 | De Opdrachtnemer dient een protocol voor back-up en recovery, conform paragraaf 2.10 “Maatregelen Back-ups” en conform de bijlage CSR 18 "Back-up en Recovery" van de bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, op te stellen en te leveren aan de Opdrachtgever. |
| 16.1.5VSP13 | De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie, te handelen. |
| 16.1.5VSP14 | De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven (Incident Response Plan), conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie een Incident Response Plan op te stellen. |
| 12.3.1VSE19 | De integriteit en beschikbaarheid van de ICT en IA van het beheerobject dient geborgd te zijn doormiddel van back-ups conform paragraaf 2.10 "Maatregelen back-ups" en bijlage CSR 18 "Back-up en recovery" van de [Cybersecurity Implementatierichtlijn Objecten]. |
| 16.1.5VSE39 | De ICT en IA van het beheerobject dient naar een vooraf gedefinieerde veilige situatie gestuurd te worden in geval van een aanval, incident of calamiteit conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. Periodieke beproevingen

[beschrijf op welke wijze de continuïteitsplannen, Het INciDEnt responseplan en de RECOVERY plannen en het BACK-UP en RECOVERY proces periodiek worden getest en geactualiseerd.]

|  |  |
| --- | --- |
| 17.2.2VSP59 | De Opdrachtnemer dient een continuïteitsplan voor energievoorziening op te stellen conform de bijlage CSR 12 "Continuïteitsplan voor energievoorziening" van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces en te leveren aan de Opdrachtgever. |
| 17.2.2VSP60 | De Opdrachtnemer dient de continuïteitsplannen voor energievoorziening die ter beschikking zijn gesteld in bijlage A “Informatie Areaal” bij de Vraagspecificatie ten minste jaarlijks uit te voeren, actueel te houden en te leveren aan de opdrachtgever. |
| 5.1.1.1VSP57 | De Opdrachtnemer dient conform bijlage CSR 15 "Recoveryplan" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, een recoveryplan op te stellen, waarmee tevens een succesvolle cyberaanval op de ICT en IA (assume breach) wordt afgedekt en te leveren aan de Opdrachtgever. |
| 12.3.1VSP58 | De Opdrachtnemer dient een protocol voor back-up en recovery, conform paragraaf 2.10 “Maatregelen Back-ups” en conform de bijlage CSR 18 "Back-up en Recovery" van de bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, op te stellen en te leveren aan de Opdrachtgever. |
| 16.1.5VSP13 | De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie, te handelen. |
| 16.1.5VSP14 | De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven (Incident Response Plan), conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie een Incident Response Plan op te stellen. |
| 12.3.1VSE19 | De integriteit en beschikbaarheid van de ICT en IA van het beheerobject dient geborgd te zijn doormiddel van back-ups conform paragraaf 2.10 "Maatregelen back-ups" en bijlage CSR 18 "Back-up en recovery" van de [Cybersecurity Implementatierichtlijn Objecten]. |

* + 1. AVG en verwerkersovereenkomst

[BESCHRIJF HOE IS GEBORGD DAT OPDRACHTNEMER IN HET KADER VAN DE AVG, DE PERSOONSGEGEVENS EN ANDERE TOT NATUURLIJKE PERSONEN HERLEIDBARE GEGEVENS, WAARONDER CAMERABEELDEN, OP RECHTMATIGE WIJZE HANDELT. Hiervoor dient eventueel een VErwerkersovereenkomst te zijn afgesloten tussen opdrachtnemer en opdrachtgever (CONFORM VERWERKERSOVEREENKOMST).]

|  |  |
| --- | --- |
| 15.1.1.318.1.4VSP19 | Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt, dan dient de Opdrachtnemer een verwerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon “verwerkersovereenkomst” dat de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt. |
| 18.1.4VSP18 | De Opdrachtnemer dient in het kader van de Algemene verordening gegevensbescherming (AVG) de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen. |

* + 1. Videocamera’s en opslag videobeelden

[BESCHRIJF OP WELKE WIJZE OPDRACHTNEMER INVULLING GEEFT AAN DE RICHTLIJN Camera’S en omgang met camerabeelden van de verkeersregistratiesystemen, INDIEN OPDRACHTNEMWER BEHEER EN ONDERHOUDSWERKZAAMHEDEN UITVOERT AAN VIDEOCAMERA’S EN/OF SYSTEMEN WAAROP CAMERABEELDEN ZIJN OPGESLAGEN.]

|  |  |
| --- | --- |
| 18.1.4VSP20 | Indien de Opdrachtnemer camera’s inzet en/of camerabeelden opslaat, verwerkt of distribueert, dan dient de Opdrachtnemer de bijlage CSR 20 "Camera's en omgang met camerabeelden van de verkeersregistratiesystemen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie, te volgen. |

* + 1. Beveiliging Spionage

[beschrijf 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.]

|  |  |
| --- | --- |
| 15.1.118.1.3VSP23 | 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, IP-tabellen, netwerkschema's, modellen, tekeningen en berekeningen, zijn beveiligd tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging. |

* + 1. Beveiliging van de Informatievoorziening

[beschrijf 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.]

|  |  |
| --- | --- |
| 8.3.2.118.1.3VSP22 | De Opdrachtnemer dient het deel van zijn informatievoorziening, dat benodigd is voor de door de Opdrachtgever gevraagde Documenten en dat benodigd is bij de verwerking van de door de Opdrachtgever ter beschikking gestelde informatie, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging. |
| 8.3.2.2VSP24 | De Opdrachtnemer dient uiterlijk bij beëindiging van de Overeenkomst alle Documenten en door de Opdrachtgever ter beschikking gestelde informatie die kwetsbaarheden kunnen veroorzaken voor de Opdrachtgever en die niet eerder zijn overgedragen alsnog over te dragen aan de Opdrachtgever. Datgene wat is overgedragen en wat niet wordt of niet kan worden overgedragen, dient te worden gewist en/of vernietigd in de informatievoorziening van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst. |
| 8.3.2.2VSP25 | Indien de Opdrachtnemer ICT- en IA-componenten en/of de daarop aanwezige informatie verwijdert, hergebruikt en/of vernietigt, dan dient hij conform de bijlage CSR 23 "Verwijdering en vernietiging van informatie en apparatuur" van bijlage V "Cybersecurity Implementatierichtlijn objecten" bij deze Vraagspecificatie Proces, te handelen. |

* + 1. Cybersecurity wet- en regelgeving

[BESCHRIJF OP WELKE WIJZE OPDRACHTNEMER ZICH OP DE HOOGTE STELT VAN VERANDERENDE WET- EN REGELGEVING RELEVANT VOOR CYBERSECURITY EN ZICHT HIERAAN HOUDT BINNEN DE EIGEN OMGEVING

EVENTUELE CONSEQUENTIES VOOR OPDRACHTGEVER DIENEN TE WORDEN GERAPPORTEERD.]

|  |  |
| --- | --- |
| 18.1.2VSP48 | De Opdrachtnemer dient voor het intellectueel eigendomsrecht, gebruiksrecht en Escrow van software voor ICT en IA de bijlage CSR 19 "Intellectueel Eigendom" van bijlage V “Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie, te volgen. Opdrachtgever bepaalt op basis van een risico afweging tot inzet van Escrow. |

* + 1. Gelaagde beveiliging

[BESCHRIJF OP WELKE WIJZE INVULLING IS GEGEVEN AAN HET PRINCIPE VAN GELAAGDE BEVEILIGING VAN DE ICT EN IA.]

|  |  |
| --- | --- |
| 5.1.1.1VSE03 | De ICT en IA van het beheerobject dient zodanig te zijn gerealiseerd dat de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging is ingericht. |

* + 1. Plaatsing en bescherming van ICT en IA

[BESCHRIJF OP WELKE WIJZE DE ICT EN IA WORDEN BESCHERMD TEGEN SCHADE, STORING EN OMGEVINGSINVLOEDEN (B.V. WATER, VUUR, ROOK, STRALING, IMPACT, CORROSIE.]

|  |  |
| --- | --- |
| 11.1.4VSE12 | ICT en IA van het beheerobject dient tegen schade en storing beschermd te zijn. |

|  |  |
| --- | --- |
| 11.1.411.2.6VSE13 | De ICT en IA van het beheerobject dient, indien geplaatst buiten beveiligde gebouwen en ruimten, op basis van een risico analyse en afweging geplaatst te zijn in afsluitbare kasten of ruimten, die bij fysieke opening een alarmmelding genereren, die opgevolgd wordt, evenals bij ongeautoriseerde logische toegang tot het datanetwerk in de kast of ruimte. |

* + 1. Voedings- en communicatiekabels

[BESCHRIJF OP WELKE WIJZE VOEDINGS- EN COMMUNICATIEKABELS DIE VOOR DATAVERKEER OF ONDERSTEUNENDE INFORMATIEDIENSTEN WORDEN TOEGEPAST, WORDEN BESCHERMD TEGEN AFTAPPEN EN BESCHADIGING.]

|  |  |
| --- | --- |
| 11.2.111.2.3VSE14 | Voedings- en telecommunicatiekabels van het beheerobject die voor dataverkeer of ondersteunende informatiediensten zijn toegepast dienen tegen interceptie, verstoring of schade beschermd te zijn. |

* + 1. Validatie controles

[BESCHRIJF OF, EN OP WELKE WIJZE, IN ALLE GEVALLEN IS VOLDAAN AAN INPUT EN OUTPUT VALIDATIE, OM EVENTUEEL CORRUMPEREN VAN INFORMATIE DOOR VERWERKINGSFOUTEN OF OPZETTELIJKE HANDELINGEN TRACEERBAAR TE MAKEN.]

|  |  |
| --- | --- |
| 14.1.1VSE31 | ICT en IA van het beheerobject dient voorzien te zijn van invoer en uitvoer validatie controles om corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken. |

1. Incidentproces, SOC meldingen en verhoogde dreiging en Recovery

[beschrijf hier welk proces er is ingericht en wordt gevolgd voor security incidenten en meldingen van het SOC 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.]

|  |  |
| --- | --- |
| 5.1.1.1VSP57 | De Opdrachtnemer dient conform bijlage CSR 15 "Recoveryplan" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, een recoveryplan op te stellen, waarmee tevens een succesvolle cyberaanval op de ICT en IA (assume breach) wordt afgedekt en te leveren aan de Opdrachtgever. |
|  |  |
| 16.1.2.416.1.3VSP03 | De Opdrachtnemer dient de hierna volgende inhoudsopgave van de voortgangsrapportage nader af te stemmen met de Opdrachtgever.1. Projectmanagement:e. security incidenten conform de bijlage CSR 21 “Uniform aanleveren van incidentrapportages” van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces; |
| 16.1.3.1VSP06 | De opdrachtnemer dient een proces in te richten voor het ontvangen van meldingen van kwetsbaarheden van buitenaf conform de "Leidraad Coordinated Vulnerability Disclosure" van het Nationaal Cyber Security Centrum. |
| 16.1.5VSP13 | De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij de Vraagspecificatie, te handelen. |
| 16.1.5VSP14 | De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en tevens een Incident Response Plan conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces op te stellen. |
| 16.1.6VSP15 | De Opdrachtnemer dient de opgetreden cybersecurity incidenten te analyseren en maatregelen te treffen om herhaling te voorkomen. De Opdrachtnemer dient jaarlijks alle cybersecurity incidenten te analyseren en deze rapportage op te nemen in het cybersecurity dossier. |
| 16.1.6.1VSP16 | De Opdrachtnemer dient een proces inzake 'probleembeheer' te beschrijven zodanig dat security incidenten, waarvoor nog geen oplossing beschikbaar is, worden beheerst en zodanig dat op proactieve wijze nieuwe incidenten kunnen worden voorkomen en/of de gevolgen daarvan worden beperkt. |
| 16.1.7VSP17 | De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal. |

1. Cybersecurity audit
	1. Bevindingen

[beschrijf de bevindingen die voortvloeien uit de jaarlijkse audit.]

|  |  |
| --- | --- |
| 18.2.1.1VSP65 | De Opdrachtnemer dient de cybersecurity eisen integraal onderdeel te maken van het projectmanagementsysteem en of Information Security Management Systeem (ISMS). |
| 18.2.1.1VSP66 | De Opdrachtnemer dient het projectmanagementsysteem met geplande tussenpozen te beoordelen, om te bewerkstelligen dat dit bij voortduring geschikt, passend en doeltreffend is. |
| 18.2.1.1VSP67 | De Opdrachtnemer dient te meten, te analyseren en te verbeteren zodanig dat het projectmanagementsysteem doeltreffend functioneert. |
| 18.2.1.1VSP68 | De Opdrachtnemer dient negatieve bevindingen en tekortkomingen die door de Opdrachtgever zijn geconstateerd en gemeld aan de Opdrachtnemer, af te handelen op gelijke wijze als afwijkingen die door de Opdrachtnemer zijn geconstateerd. |
| 5.1.1.1VSP12 | De Opdrachtnemer dient ten minste één keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de auditrapportage ter kennis te brengen van de Opdrachtgever. |
| 18.2.2VSP69 | De Opdrachtnemer dient de zelfstandige hulppersonen te managen, zodanig dat wordt gewaarborgd dat de door zelfstandige hulppersonen verrichte Werkzaamheden en de resultaten daarvan voldoen aan de eisen voorvloeiende uit de Overeenkomst. |

* 1. Risico’s

[beschrijf de risico’s in relatie tot de bevindingen uit de voorafgaande paragraaf.]

* 1. Aanbevelingen en verbetermaatregelen

[beschrijf de aanbevelingen en de verbetermaatregelen naar aanleiding van de bevinding en hieraan gerelateerde risico’s.]

1. Cybersecurity Incident Response- en rapportageproces
	1. Beveiligingsincidenten

[beschrijf de inrichting en werking van het Cybersecurity incident RESPONSe proces en het RAPPORTAGE proces langs de door Opdrachtgever aangereikte format en criteria. Een jaaroverzicht wordt door Opdrachtnemer opgesteld om analyse van de incidenten mogelijk te maken.]

|  |  |
| --- | --- |
| 16.1.2.416.1.3VSP03 | De Opdrachtnemer dient de hierna volgende inhoudsopgave van de voortgangsrapportage nader af te stemmen met de Opdrachtgever.1. Projectmanagement:e. security incidenten conform de bijlage CSR 21 “Uniform aanleveren van incidentrapportages” van bijlage V “Cybersecurity Implementatierichtlijn Objecten” bij deze Vraagspecificatie Proces; |
| 16.1.5VSP13 | De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |
| 16.1.5VSP14 | De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven, conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en tevens een Incident Response Plan conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces op te stellen. |
| 16.1.6VSP15 | "De Opdrachtnemer dient de opgetreden cybersecurity incidenten te analyseren en maatregelen te treffen om herhaling te voorkomen. De Opdrachtnemer dient jaarlijks alle cybersecurity incidenten te analyseren en deze rapportage  op te nemen in het cybersecurity dossier. |

* 1. Risico’s

[beschrijf de analyse resultaten van de Cybersecurity beveiligingsincidenten die beschreven staan in de voorgaande paragraaf.]

* 1. Aanbevelingen en verbetermaatregelen

[beschrijf de verbetermaatregelen die reeds zijn getroffen naar aanleiding van –of voortvloeien uit- de uitgevoerde analyse uit de voorgaande paragraaf.]

1. Security gerelateerde wijzigingen
	1. Security gerelateerde wijzigingen

[beschrijf op welke wijze security gerelateerde wijzigingen worden beoordeeld op mogelijke impact en risico’s alvorens de wijziging wordt doorgevoerd. OPDRACHGEVER kan dit soort wijzigingen aankondigen via riskletters of notes]

|  |  |
| --- | --- |
| 12.1.2VSP49 | De Opdrachtnemer dient met betrekking tot het doorvoeren van Wijzigingen aan bestaande ICT en IA, conform paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen. |
| 12.6.1.1VSP53 | Indien de Opdrachtgever melding maakt van een kritieke of niet kritieke patch dan dient de Opdrachtnemer daarvoor een implementatieadvies  ter kennis te brengen van de Opdrachtgever. Daarbij gelden de volgende doorlooptijden: 1.    voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;2.    voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever. De Opdrachtnemer dient de patch, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren. |
| 12.6.1VSP51 | De Opdrachtnemer dient met betrekking tot het patchen van de ICT en IA, conform paragraaf 2.5 “Maatregelen bescherming tegen kwetsbaarheden” en conform de bijlage CSR 8 “Patch management" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te handelen. |

* 1. Overzicht security gerelateerde wijzigingen

[beschrijf de security gerelateerde wijzingen die conform de overeenkomst aan Opdrachtgever zijn gerapporteerd.

* 1. Analyse security gerelateerde wijzigingen en aanbevelingen

[beschrijf de resultaten van de uitgevoerde analyse van de security gerelateerde wijzigingen en geeft aan of er aanbevelingen zijn.]

1. Evaluatie en actualisatie van risico’s en beheersmaatregelen
	1. Risicoanalyse en risicoafweging

[beschrijf de resultaten van de door Opdrachtnemer uitgevoerde risicoanalyse (conform de eis uit de overeenkomst of de Cybersecurity Implementatierichtlijn Objecten) en de risicoafweging die is gemaakt.]

|  |  |
| --- | --- |
| 5.1.1.VSP01 | De Opdrachtnemer dient de Werkzaamheden met betrekking tot cybersecurity zodanig te verrichten dat het gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen. |
| 5.1.1.1VSP02 | De Opdrachtnemer dient zijn procesbeschrijving (cybersecurity plan) , waarmee invulling wordt gegeven aan de bovenliggende eis VSP01 en ten minste aan alle daaraan onderliggende eisen, ter kennis te brengen van de Opdrachtgever. |
| 14.1.1.1VSP04 | De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever. |
| 14.2.6.1VSP061 | Indien de Opdrachtnemer Werkzaamheden door zelfstandige hulppersonen wil laten verrichten, dan dient de Opdrachtnemer een quickscan conform de handleiding "Quickscan nationale veiligheid bij inkoop en aanbesteden" uit te voeren en het resultaat ter kennis te brengen van de Opdrachtgever. |

* 1. Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen

[beschrijf de resultaten van de jaarlijkse beproevingen van het back-up en recovery proces, Het RECOVERY PLan en de continuïteitsplannen en voorzieningen en geef aan of er verbeteringen noodzakelijk zijn.]

* 1. Cybersecurity beheersmaatregelen

[beschrijf de verbetermaatregelen die voortvloeien uit de door OPDRACHTNEMER periodiek uitgevoerde risicoanalyse en risicoafweging.]

1. Verklaring Opdrachtnemer
	1. Risicoanalyse en risicoafweging

[geef 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.]

1. Bijlagen
	1. Relevante bijlagen

[voeg hier de relevante bijlagen toe met een korte toelichting voor elke bijlage.]

1. IEC 62443 is de internationale norm voor cybersecurity van Industriële Automatisering en Controle Systemen. [↑](#footnote-ref-1)
2. Zie bijvoorbeeld paragraaf 1.2. [↑](#footnote-ref-2)
3. Zie bijvoorbeeld paragraaf 2.1.1. [↑](#footnote-ref-3)