Bijlage 8. Standaard OT-security eisen

CS01	De Opdrachtnemer dient de werkzaamheden en de daarbij behorende processen, met betrekking tot cybersecurity, zodanig te verrichten en de ICT en IA van het beheerobject zodanig in te richten, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.
CS02	De Opdrachtnemer dient zijn procesbeschrijving (cybersecurity plan), waarmee invulling wordt gegeven aan de bovenliggende eis en te minste aan alle daaraan onderliggende eisen, ter kennis brengen van de Opdrachtgever. Voor het opstellen van het cybersecurity plan dient de Opdrachtnemer het door de Opdrachtgever ter beschikking gestelde template te gebruiken. Dit plan dient zowel voor als na de werkzaamheden te worden opgeleverd aan de Opdrachtgever. Voor de uitvoering van de werkzaamheden beschrijft het de geplande implementatie en na uitvoering beschrijft het de daadwerkelijke implementatie van de maatregelen. Gedurende de werkzaamheden dient het cybersecurity plan actueel te worden gehouden en op verzoek aangeleverd te worden aan de Opdrachtgever.
CS03	De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de werkzaamheden met betrekking tot cybersecurity en alle taken, rollen en bevoegdheden betrokken bij de werkzaamheden te communiceren met de Opdrachtgever.
CS04	De Opdrachtnemer dient voor alle beheerobjecten evenals de ICT en IA van de beheerobjecten de van toepassing verklaarde maatregelen uit de Cybersecurity Implementatierichtlijn Objecten 3.4 (CSIR) uit te voeren die behoren bij cybersecurity weerstandsniveau 1 tenzij er voor het beheerobject een ander cybersecurity weerstandsniveau is overeengekomen. - Beheerobject x – cybersecurity weerstandsniveau x
CS05	Indien de Opdrachtnemer tijdelijk niet aan de eisen 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.
CS06	De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.
CS07	De Opdrachtnemer dient alle opdracht gerelateerde informatie — zowel door de Opdrachtgever verstrekte documenten als door de Opdrachtnemer zelf geproduceerde gegevens — zodanig beveiligen dat deze zijn beschermd tegen verlies, ongeautoriseerde toegang en ongeoorloofde wijzigingen. Daarnaast treft de Opdrachtnemer, op basis van een risicoanalyse, passende maatregelen tegen spionage. Deze maatregelen waarborgen dat ICT- en IA-gerelateerde documenten, waaronder documentatie, offertes, contracten, tekeningen en berekeningen, adequaat zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijzigingen.
CS08	De Opdrachtnemer dient uiterlijk bij beëindiging van de overeenkomst alle documenten en door de opdrachtgever ter beschikking gestelde informatie over te dragen aan de Opdrachtgever. Alle informatie (voor zover bewaring niet wettelijk verplicht) dient te worden vernietigd in de informatievoorzieningen van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst. Daarnaast dient de Opdrachtnemer alle beschikbaar gestelde bedrijfsmiddelen nadat ze niet meer van dienst zijn geworden of uiterlijk bij beëindiging van de overeenkomst terug te geven.
CS09	De Opdrachtnemer dient Werkzaamheden aan het ontwerp, beheer en onderhoud evenals de gevoelige informatie en documentatie van de beheerobjecten en de hieraan gerelateerde ICT en IA door medewerkers te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en over een Verklaring Omtrent 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 medewerkers.
CS10	De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van: 1. De door de Opdrachtnemer aan de medewerkers verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen; 2. De fysieke toegang van de medewerkers tot ICT en IA gerelateerde ruimten. Deze informatie wordt gedeeld met de Opdrachtgever.
CS11	De Opdrachtnemer vereist dat al zijn medewerkers, waaronder eigen personeel, ingehuurd personeel en onderaannemers, de cybersecurity-eisen en maatregelen toepassen in overeenstemming met de door de Opdrachtgever vastgestelde beleidsregels en procedures. De Opdrachtnemer beheert en stuurt deze medewerkers zodanig aan dat wordt gewaarborgd dat de door hen verrichte werkzaamheden en de daaruit voortvloeiende resultaten volledig voldoen aan de eisen die uit de overeenkomst voortvloeien.
CS12	De Opdrachtnemer dient negatieve bevindingen en tekortkomingen die door de Opdrachtgever zijn geconstateerd en gemeld aan de Opdrachtnemer, te voorzien van passende opvolging.
CS13	Het beheerobject en de ICT en IA dienen zodanig gerealiseerd te zijn dat de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging is ingericht en tegen schade en storing zijn beschermd.
CS14	De ICT en IA van het beheerobject dient, indien geplaats buiten beveiligde gebouwen of ruimten, op basis van een risicoanalyse 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.
CS15	Voedings- en telecommunicatiekabels op het beheerobject die voor dataverkeer of ondersteunende informatiediensten zijn toegepast dienen tegen interceptie, verstoring of schade beschermd zijn.
CS16	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 securityfuncties en maatregelen. De Opdrachtnemer dient het testplan waarin de testcases worden beschreven evenals de resultaten van het testen te delen met de Opdrachtgever.
CS17	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 deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.