

Titel	CS-Eisen (Cybersecurity-eisen) MET OT (CEB-OVG-18909)
Voor uitleg:	Zie CS-Voorschrift MET OT (CEB-OVG-21876)
	Zie tabblad CS-Eisen OT MET voor de inhoud
	Deze eisenset is bedoeld om om te zetten naar vraagspecificaties als onderdeel van aanbesteding voor de ontwikkeling van een object/asset en/of is bedoeld als default-set voor het ontwerpen van cybersecuritymaatregelen van een object/asset op basis van een risicoanalyse.
	Voor het gebruik van deze CS-eisenset wordt verwezen naar CS-Voorschrift (CEB-OVG-21876)
Kolom :	Eis-type: Informatief of een Eis (Requirement)
Kolom :	Eis-type: VS-Algemeen, VS1 (systeem) of VS2 (proces)
Kolom :	Eis-Hoofdstuknummer
Kolom :	Eis-Paragraafnummer
Kolom :	Eis-Hoofdstuktitel
Kolom :	Eis-Paragraaftitel
Kolom :	Eis-Paragraaftekst / Eistekst
Kolom :	Verklaring van toepasselijkheid voor BIO, ISO27001, IEC62443, CSIR, NCSC (<i>volgt</i>)
Join:	CEB-OVG-18908
Auteur:	W.L. van Asperen, CS Officer en Privacy Officer MET OT
Vertrouwelijkheid:	Niet-vertrouwelijk
Versie:	Versie 1.2
Datum:	21-12-2020
Status:	H0 en H1: Referentie := Bindende referentie; H0 en H1: Informatief := Bindend informatief; H1 en H2: Eis-type is nu Informatief voor informatieve paragrafen; Nieuwe tekst bij H4,P4: <i>Opdrachtnemer actualiseert steeds tijdens de projectfasen het Cybersecuritydossier zoals dat is meegeleverd door de Opdrachtgever. Nieuwe tekst bij H4,P5: Opdrachtnemer laat bij het einde van elke projectfase het geactualiseerde Cybersecuritydossier goedkeuren door Opdrachtgever. Toegevoegde tekst bij H8, P2 en P3: toevoegen ...dat betrokken is bij CS; Nieuwe tekst bij H11, P3: Opdrachtnemer voorziet in een door Opdrachtgever goedgekeurde cyberrisicoanalyse voor de fysieke en/of digitale bescherming van perifere systeemonderdelen die in de publieke ruimte staan (zoals camera, liften en OVCP-poortjes); Toegevoegde tekst bij H12, P4: ...in geval van een meerjarencontract; Toegevoegde tekst bij H13, P3: ...genomen; Toegevoegde tekst bij H13, P7: ... (periodiek);</i>
Versie:	Versie 1.1
Datum:	23 januari 2020
Status:	Eisen opgenomen voor een handbediende terugvaloptie bij Herstel Eis 6 en 7
Versie:	1.0 Definitief
Datum:	17-12-2019
Status:	Reviewopmerkingen van de beide review sessies in november 2019 verwerkt; Vast te stellen door CS-Board; Vast te stellen door DT MET; Vast te stellen door MET E&B; Vast te stellen door CCB;
Versie:	0.9
Status:	Ter review
Datum review:	2 sessies in november 2019
Review door:	Peter van Gestel, Jan de Liefde, Hans Deuss, Andre van der Veen, Louis de Wolff, Daniel Wunderink (GVB)

Zie het tabblad Voorblad voor de status van dit document.

Eis-type	VS-type	Hoofdstuk-nummer	Hoofdstuk-titel	Paragraaf-nummer	Paragraaftitel	Paragraaftekst
Maatregel	VS-Algemeen	0	Uitleg	0	Unieke nummering van de eisen/maatregelen	De eis/maatregeltekst is uniek genummerd door hoofdstuknummer en Paragraafnummer. Voorbeeld: (2, 20, Definitie, De Operatie) of (13, 9, Hardening, Testen van apparatuur)
Bindend informatief	VS-Algemeen	1	Bindende referentie	1	CybersecurityVoorschrift	CybersecurityVoorschrift MET OT is het top-document aangaande de cybersecurity, Join CEB-OVG-21876.
Bindend informatief	VS-Algemeen	1	Bindende referentie	2	Risicomanagementaanpak	CS-Risicomanagementaanpak OT MET, CEB-OVG-18786
Bindend informatief	VS-Algemeen	1	Bindende referentie	3	Dreigingsbeeld	CS-Dreigingsbeeld OT MET, CEB-OVG-22124 (Zeer-vertrouwelijk)
Bindend informatief	VS-Algemeen	1	Bindende referentie	4	Cybersecuritydossiersjabloon	Cybersecuritydossiersjabloon voor OT MET, CEB-OVG-20265
Bindend informatief	VS-Algemeen	1	Bindende referentie	5	Cybersecuritybeleid	Cybersecuritybeleid MET OT, CEB-OVG-20961
Bindend informatief	VS-Algemeen	1	Bindende referentie	6	Cybersecurity KPI's	Cybersecurity KPI's MET OT, CEB-OVG-21172
Bindend informatief	VS-Algemeen	1	Bindende referentie	7	Vertrouwelijkheid	Vertrouwelijkheid MET OT, CEB-OVG-20264
Bindend informatief	VS-Algemeen	1	Bindende referentie	8	Incidentmanagement	Integrale Incidentmanagementprocedure OT Metro en Tram, CEB-OVG-18784
Bindend informatief	VS-Algemeen	1	Bindende referentie	9	Aansluitvoorwaarde NMA	Aansluitvoorwaarden van het NMA, CEB-OVG-21512
Bindend informatief	VS-Algemeen	1	Bindende referentie	10	Hardeningvoorschrift	Hardening voor OT MET, CEB-OVG-21203
Bindend informatief	VS-Algemeen	1	Bindende referentie	11	Wachtwoordenbeleid	Wachtwoordenbeleid MET OT, CEB-OVG-21794
Bindend informatief	VS-Algemeen	1	Bindende referentie	12	Checklist OT NCSC	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/checklist-beveiliging-ics-scada
Bindend informatief	VS-Algemeen	2	Definitie	1	Voorwaardelijk	Voorwaardelijke bepalingen zijn bepalingen die noodzakelijk en toepasselijk zijn voor Cybersecurity. Voorbeelden zijn bepalingen die betrekking hebben op configuratiebeheer en fysieke toegangsbeheer. Deze dienen elders in de vraagspecificatie geformuleerd te zijn en zijn dan ook voor cybersecurity toepasselijk. Tegenstrijdigheden dienen met Opdrachtgever besproken te worden. Opdrachtgever geeft dan duiding.
Bindend informatief	VS-Algemeen	2	Definitie	2	RAMSSHEEP	Cybersecurity is een systeemaspect, net als onderhoudbaarheid, duurzaamheid en veiligheid. De systeemaspecten zullen elkaar onderling beïnvloeden, of misschien elkaar onderling beconcurreren. Cybersecurity is onderhevig aan een keuzeproces in het (gefaseerde) systeemontwerp om te komen tot een optimaal cybersecurityontwerp cq gebalanceerde set aan cybersecuritymaatregelen. Voor de OT van MET geldt het keuze- c.q. ontwerpproces op basis van risicoanalyse en zoals gegeven in de referenties Risicomanagementaanpak en CybersecurityVoorschrift.
Bindend informatief	VS-Algemeen	2	Definitie	3	Cybersecurity	Cybersecurity is het continu beheersen van cyberrisico's door incidenten te voorkomen en/of (de impact van) restrisico's te mitigeren (tot en met het herstellen van systemen en operatie), die kunnen leiden tot (im)materiële schade en/of letsel aan alle stakeholders. De doelstelling van cybersecurity is gegeven bij de Doelstelling Top-Doel. Zie ook referentie Cybersecuritybeleid MET
Bindend informatief	VS-Algemeen	2	Definitie	4	Cyberincident	Een cyberincident is (kans op) een (on)bedoelde inbreuk op de a. de vertrouwelijkheid van informatie, b. de integriteit van informatie en systeemgedrag, c. de beschikbaarheid van informatie en systeemgedrag. Zie Referentie Incidentmanagement
Bindend informatief	VS-Algemeen	2	Definitie	5	Cybersecuritydossier	Het Cybersecuritydossier beschrijft voor het Systeem de cybersecurity: doelen, eisen, risicoanalyses (en restrisico's) en gerelateerde voorzieningen en maatregelen; vanuit het van de dagelijkse operatie (exploitatie en onderhoud). Het Cybersecuritydossier van het Systeem is ontwerpdocument en wordt tijdens de projectfasen en tijdens de beheerfasen nader ingevuld en geactualiseerd. Het Cybersecuritydossier wordt opgesteld op basis van de referentie Cybersecuritydossiersjabloon.
Bindend informatief	VS-Algemeen	2	Definitie	6	Classificatiegestuurde en Risicogestuurde maatregelen	Cybersecuritymaatregelen kunnen worden voorgeschreven op basis van vaste beveiligingsniveau's. Het beveiligingsniveau voor een Systeem wordt dan veelal bepaald aan de hand van een gegeven risicochecklist (zoals de VRA) of wordt voorgeschreven door de opdrachtgever. Cybersecuritymaatregelen kunnen ook op basis van een risicoanalyse van het Systeem in de beoogde operationele omgeving worden samengesteld, waarbij een standaard maatregelenset het uitgangspunt is. De risicoanalyse geeft dan de onderbouwing voor de comply-or-explain van de standaard maatregelenset. Het beleid van MET voor de OT is om de risicogebaseerde aanpak te hanteren: zie de referentie Risicomanagementaanpak. De compliancyonderbouwing is gegeven in Referentie CybersecurityVoorschrift.
Bindend informatief	VS-Algemeen	2	Definitie	7	Het Systeem	Met Systeem wordt bedoeld het Systeem zoals dat in de vraagspecificatie is beschreven en wat het onderwerp is van de cybersecurity.
Bindend informatief	VS-Algemeen	2	Definitie	8	Type Operationele Technologie (OT)	Het Systeem is een systeem van het type Operationele Technologie (OT) waarmee wordt bedoeld: het geheel of een onderdeel van de operationele bediening-, besturing en bewakingssystemen, bestaande uit hardware en software, zoals netwerken, verbinding- en (onderhouds-)apparatuur, ICS- SCADA-, PLC-, IO-systemen, camera's, remote controllers, vpn, intercomsystemen, bedienplekken, roltrappen, liften en sensoren en actuatoren.
Bindend informatief	VS-Algemeen	2	Definitie	9	IAA-gegevens	IAA-gegevens zijn (alle typen van) Identificatie-, Authenticatie- en Autorisatiegegevens (inclusief inloggegevens) waarmee alleen bevoegd(e) Personeel en Gebruikers toegang krijgen tot het Systeem.
Bindend informatief	VS-Algemeen	2	Definitie	10	Hardening	Hardening betreft het technisch beveiligen van het Systeem en betreft meer dan het beperken van toegang/rechten en software en rechten. Zie referentie: Hardeningvoorschrift.
Bindend informatief	VS-Algemeen	2	Definitie	11	Procedure	Met een Procedure wordt bedoeld een op schrift vastgelegde beschrijving van (een reeks van) handelingen. Een procedure kan een onderdeel zijn van een proces. Een Procedure dient bekend te zijn bij de betrokken medewerkers en te worden uitgevoerd waar dat van toepassing is.
Bindend informatief	VS-Algemeen	2	Definitie	12	Configuratie	De configuratie van het Systeem is een gestructureerd overzicht (van de versies) van de (gedecomposeerde) systeemonderdelen (configuratieitems, CI's). Cybersecurityvoorzieningen zijn ook CI's.
Bindend informatief	VS-Algemeen	2	Definitie	13	Cybersecurity-voorzieningen	Cybersecurity-voorzieningen zijn alle software en hardware voorzieningen bedoeld ter bescherming van Beschikbaarheid, Integriteit en Vertrouwelijkheid van het Systeem en de Veiligheid, Beschikbaarheid, Privacy van de Operatie.
Bindend informatief	VS-Algemeen	2	Definitie	14	Personeel	Met Personeel wordt bedoeld alle medewerkers die in opdracht van Opdrachtnemer (en haar Oderaannemers) werkzaamheden uitvoeren aan of gebruik maken van het Systeem en Toegang hebben tot de het Systeem.
Bindend informatief	VS-Algemeen	2	Definitie	15	Patches	Met een Patch wordt bedoeld een oplossing voor een versie van de software. Met Patches wordt - in deze context - bedoeld alle soorten verbeteringen (updates, updates en patches) voor de software (inclusief firmware of embedded code) die betrekking hebben op de beveiliging van het Systeem, inclusief anti-virussoftware.
Bindend informatief	VS-Algemeen	2	Definitie	16	Meldpunt	Meldpunt Cybersecurity Officer OT MET

Zie het tabblad Voorblad voor de status van dit document.

Eis-type	VS-type	Hoofdstuk-nummer	Hoofdstuk-titel	Paragraaf-nummer	Paragraaftitel	Paragraaftekst
Bindend informatief	VS-Algemeen	2	Definitie	17	Herstel	Herstel betreft alle maatregelen (processen en voorzieningen) gericht op het kunnen herstellen van het Systeem na een cyberincident, dus inclusief backup, compromise assessing en restore.
Bindend informatief	VS-Algemeen	2	Definitie	18	Cyberincidentmanagement	Cyberincident management betreft alle stappen in het afhandelen van een incident: vanaf de melding, oorzaakanalyse, eventueel zekerstellen van bewijsmateriaal, herstellen van het Systeem en het herstellen van de Operatie, inclusief het managen ervan (CSIRT).
Bindend informatief	VS-Algemeen	2	Definitie	19	Configuratiebeheer	Configuratiebeheer is het actueel houden en vaststellen van configuraties van het Systeem. Configuratiebeheer is randvoorwaardelijk voor de cybersecurity.
Bindend informatief	VS-Algemeen	2	Definitie	20	De Operatie	De Operatie betreft alle dagdagelijkse en tactische werkzaamheden voor de exploitatie, voor het beheer en onderhoud en eventuele calamiteiten met het Systeem door Personeel en de medewerkers van Opdrachtgever en Hulpdiensten.
Bindend informatief	VS-Algemeen	3	Doelstelling	1	Top-doel	Cybersecurity's doel is het faciliteren van de operationele Veiligheid, Beschikbaarheid en Privacy ter bescherming tegen (im)materiële schade en letsel van de stakeholders door het beheersen van Beschikbaarheid, Integriteit en Vertrouwelijkheid van het Systeem(gedrag) en de informatie.
Bindend informatief	VS-Algemeen	3	Doelstelling	2	Beschikbaarheid als operationeel doel en systeemdoel	Het is het doel van cybersecurity om de gestelde eisen aan Beschikbaarheid van De Operatie te faciliteren of - op zijn minst - niet negatief te beïnvloeden. Onderliggend daaraan faciliteert de Systeem-Beschikbaarheid de Operationele Beschikbaarheid. Het onderscheid tussen de Beschikbaarheid van de Operatie en de Beschikbaarheid van het Systeem is uiteengezet in referentie Cybersecurity KPI's.
Bindend informatief	VS-Algemeen	3	Doelstelling	3	Veiligheid als operationeel doel	Het is het doel van cybersecurity om de gestelde eisen aan veiligheid te faciliteren of niet negatief te beïnvloeden. Veiligheid betreft alle vormen van veiligheid (niet limitatief): zoals spoorveiligheid, sociale veiligheid, publieksveiligheid, arbo-veiligheid, milieuveiligheid en tunnelveiligheid.
Bindend informatief	VS-Algemeen	3	Doelstelling	4	Privacy als operationeel doel	Het is het doel van cybersecurity is om de gestelde eisen aan de privacy te faciliteren of niet negatief te beïnvloeden. Privacy betreft de bescherming van persoonsgegevens en de rechten van alle betrokken personen: publiek en Personeel.
Bindend informatief	VS-Algemeen	3	Doelstelling	5	BIV als Systeemoelen	Opdrachtnemer draagt zorg dat de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid) van het Systeem én de gegevens wordt beschermd - op zijn minst - niet degradeert, ter voorkoming van (im/materiële) schade en letsel van betrokken stakeholders. Zie document Cybersecurity KPI's.
Bindend informatief	VS-Algemeen	3	Doelstelling	6	KPI-typering	Het maximum aantal operationele incidenten per jaar die leiden tot fysieke merkbare (schade en letsel) incidenten, zijn de te accepteren risico's als een gevolg van cybersysteemfalen worden door de Opdrachtgever vastgesteld aan de hand van de VUS/BOGT-matrix: - maximaal [u] van het VUS/BOGT-type: Klein en/of Middel, zonder lichamelijk letsel; - maximaal [v] van het VUS/BOGT-type: Groot en Zeer groot, zonder lichamelijk letsel; - maximaal [w] met lichamelijk letsel Deze kpi-typering dient door de Opdrachtgever te worden geconcretiseerd bij doelstelling 'KPI's'. Zie referentie Cybersecurity KPI's.
Eis	VS-Algemeen	3	Doelstelling	7	KPI's	Voor de operationele doelen van het Systeem, gerelateerd aan cybersecurity zijn de volgende KPI's vastgesteld (door Opdrachtgever vooraf vast te stellen): [u] = ...#aantal fysieke schade- of letselincidenten; [v] = ...#aantal fysieke schade- of letselincidenten; [w] = ...#aantal fysieke schade- of letselincidenten; Zie definitie KPI-typering en zie referentie Cybersecurity KPI's.
Eis	VS2	4	Algemeen	1	Proces	Opdrachtnemer treft maatregelen en realiseert voorzieningen die er voor zorgen dat de operationele doelen worden gehaald. Zie VS1, Doelstelling, KPI en document Cybersecurity KPI's.
Eis	VS2	4	Algemeen	2	Vertrouwelijkheid	Opdrachtnemer dient het opslaan, registreren, bewerken en distribueren van informatie over de cybersecurity van het Systeem zeer vertrouwelijk te behandelen en overeenkomstig beveiligd op te slaan volgens Referentie Vertrouwelijkheid.
Eis	VS2	4	Algemeen	3	Risico-analyse	Opdrachtnemer dient voor het opstellen van risico-analyses gebruik te maken van de Risicomanagementaanpak
Eis	VS2	4	Algemeen	4	CS-dossier voor Systeem	Opdrachtnemer stelt voor het Systeem een Cybersecuritydossier op basis van het Cybersecuritydossiersjabloon
Eis	VS2	4	Algemeen	5	CS-dossier goedkeuren	Opdrachtnemer laat bij het einde van elke projectfase het Cybersecuritydossier goedkeuren door Opdrachtgever.
Eis	VS2	4	Algemeen	6	Afwijken	Opdrachtnemer mag afwijken van deze eisen op basis van een schriftelijke risicoanalyse en expliciete goedkeuring door Opdrachtgever. Afwijkingen en besluiten worden vastgelegd in Cybersecuritydossier van het Systeem
Eis	VS2	4	Algemeen	6	Onderaanneming	Opdrachtnemer zorg ervoor dat alle eisen voorzieningen, procedures en voorschriften 1op1 ook van toepassing zijn voor haar (sub)onderaannemers.
Eis	VS2	4	Algemeen	8	Openheid	Opdrachtnemer levert op verzoek van Opdrachtgever alle informatie betreffende de (cyber)security, eenmalig of periodiek, in een nog af te spreken formaat. Informatie betreft de procedures, plannen, configuratieinformatie, overzichten, logs zoals genoemd in deze eisenset.
Eis	VS2	4	Algemeen	9	Recht op controle	Opdrachtgever heeft het recht om (aangekondigd en onaangekondigd) controles uit te voeren op de naleving van alle procedures en instructies van de Opdrachtnemer en/of het bepalen van de status van de cybersecurity. Opdrachtnemer zal hieraan meewerken. Controles kunnen ondermeer inspecties, mystery guest, audits, (pen-)testen of assessments zijn. Dit recht heeft geen invloed op de garantiestelling, tenzij de controle aantoonbaar heeft geleid tot degradatie van het Systeem. Controles worden door Opdrachtgever in (vrijwel) alle gevallen in samenwerking met Opdrachtnemer gepland en uitgevoerd.
Eis	VS2	4	Algemeen	10	Versleuteling	Opdrachtnemer voorziet (alle Koppelingen binnen en naar) het Systeem en gerelateerde beheersysteem (zoals voor configuratie, IAA-, sleutels) van encryptie van minstens AES-256
Eis	VS2	5	Privacy	1	Handelen conform de AVG	Opdrachtnemer handelt conform de AVG voor het Systeem waarmee Persoonsgegevens worden verwerkt met Opdrachtgever, autoriteiten, onderaannemers, nevenopdrachtnemers en Betrokkenen.
Eis	VS2	5	Privacy	2	Verwerkingsovereenkomsten	Opdrachtnemer draagt zorg voor verwerkersovereenkomst(en) en subverwerkersovereenkomst(en) conform de AVG met Opdrachtgever en betrokken onderaannemers voor die delen van Systeem waarin persoonsgegevens worden verwerkt.
Eis	VS2	6	V&V	1	Verificatie	Opdrachtnemer toont vooraf aan de inbedrijfstelling aan dat het aan alle VS1 en VS2 eisen voor Cybersecurity voldoet.
Eis	VS2	6	V&V	2	Aantoning in CS-plan	Opdrachtnemer neemt de aantoning van de VS1 en VS2 eisen op in het Cybersecuritydossier.
Eis	VS2	6	V&V	3	Validatie tegen Operationele Doelen	Opdrachtnemer toont aan dat de cybersecurity de operationele doelen Veiligheid, Beschikbaarheid en Privacy faciliteert en legt dit vast in het Cybersecuritydossier. Zie Referentie Doelstelling KPI's, Definitie Definitie KPI-typering en Definitie Beschikbaarheid Operatie v.s. Systeem.
Eis	VS2	6	V&V	4	Validatie tegen Systeemoelstellingen	Opdrachtnemer toont aan dat de cybersecurity van de systeemoelen Beschikbaarheid, Integriteit en Vertrouwelijkheid faciliteert en legt dit vast in het Cybersecuritydossier. Zie Referentie Doelstelling KPI's, Definitie Definitie KPI-typering en Definitie Beschikbaarheid Operatie v.s. Systeem.

Zie het tabblad Voorblad voor de status van dit document.

Eis-type	VS-type	Hoofdstuk-nummer	Hoofdstuk-titel	Paragraaf-nummer	Paragraaftitel	Paragraaftekst
Eis	VS2	6	V&V	5	Evaluatie	Opdrachtnemer evalueert minstens jaarlijkse de risico's en effectieve werking van de maatregelen zoals beschreven Cybersecuritydossier en stelt dit bij in overleg met de Opdrachtgever (PDCA).
Eis	VS2	7	Bewustzijn	1	Cursusmateriaal	Opdrachtnemer zorgt voor relevante cursusmateriaal voor Personeel. Relevant zijn de onderwerpen genoemd in dit document CS-Eisen.
Eis	VS2	7	Bewustzijn	2	Op peil houden	Opdrachtnemer zorgt er voor dat Personeel (periodiek) cybersecurity cursusmodulen volgt voor (het op peil houden van) het kennisniveau (behorend bij de rol).
Eis	VS2	7	Bewustzijn	3	Vertrouwelijk	Opdrachtnemer dient alle getekende Vertrouwelijkheidsverklaringen (Zie Vertrouwelijkheid) van al het Personeel actueel te beheren.
Eis	VS2	7	Bewustzijn	4	Werkoverleg	Opdrachtnemer bespreekt in werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd en wat beter kan in de toekomst.
Eis	VS2	7	Bewustzijn	5	Werkoverleg	Opdrachtnemer evalueert tijdens werkoverleggen de feedback van bewustwordingsactiviteiten- en trainingen ten aanzien van cybersecurity.
Eis	VS2	8	Personeel	1	VOG	Opdrachtnemer laat Werkzaamheden alleen door VOG-gescreend Personeel uitvoeren.
Eis	VS2	8	Personeel	2	Vertrouwelijkheidsverklaring	Opdrachtnemer komt met al het Personeel dat betrokken is bij CS een getekende Vertrouwelijkheidsverklaring overeen.
Eis	VS2	8	Personeel	3	Verantwoordelijkheden	Opdrachtnemer laat Personeel dat betrokken is bij CS schriftelijk en mondeling weten wat hun verantwoordelijkheden en bevoegdheden zijn tav cybersecurity
Eis	VS2	8	Personeel	4	Privacy	Opdrachtnemer laat Personeel weten dat hun systeemactiviteiten worden gelogd.
Eis	VS2	8	Personeel	5	Functioneren	Opdrachtnemer dient Cybersecurity op te nemen in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
Eis	VS2	8	Personeel	6	Disciplinair	Opdrachtnemer dient erop toe te zien dat bij misbruik van accounts en autorisaties disciplinaire maatregelen te worden genomen en laat dit het Personeel weten.
Eis	VS2	8	Personeel	7	Bedrijfsmiddelen	Opdrachtnemer ziet er op toe dat Personeel bedrijfsmiddelen van Opdrachtgever die ze in hun bezit hebben retourneren bij beëindiging van hun inzet, dienstverband, contract of overeenkomst.
Eis	VS2	9	Configuratiebeheer	1	Actueel configuratiebeheer	Opdrachtnemer beheert - en houdt actueel - de onderdelen van het Systeem (Configuratie Items (CI's)) inclusief de instellingen (parameters).
Eis	VS2	9	Configuratiebeheer	2	Aantonen	Opdrachtnemer toont jaarlijks aan in het cybersecuritydossier dat het configuratiebeheer actueel is.
Eis	VS2	9	Configuratiebeheer	2	Wijzigingsprocedure	Opdrachtnemer hanteert een schriftelijke procedure voor het doorvoeren en (laten) accorderen van wijzigingen aan het Systeem.
Eis	VS2	9	Configuratiebeheer	3	Risicoanalyse	Opdrachtnemer hanteert voor wijzigingen aan het Systeem een risicoanalyse voor de nieuwe situatie en voor tijdens het wijzigen.
Eis	VS2	9	Configuratiebeheer	4	Risicoanalyse	Opdrachtnemer neemt (een verwijzing naar) (de risicoafweging bij) de risico-analyses en de daaruit voortvloeiende restrisico 's en mitigatiemaatregelen op in het cybersecuritydossier van het Systeem.
Eis	VS2	9	Configuratiebeheer	5	Autorisatie	Opdrachtnemer ziet er op toe dat wijzigingen alleen door geautoriseerd Personeel worden aangevraagd, gepland en uitgevoerd.
Eis	VS2	9	Configuratiebeheer	6	Beveiligingsupdates	Opdrachtnemer zorgt er voor dat updates en patches via de wijzigingsprocedure verlopen.
Eis	VS2	9	Configuratiebeheer	7	Testen vooraf	Opdrachtnemer dient wijzigingen in het Systeem vooraf aan de implementatie in productie te controleren/testen dat er geen nadelige gevolgen zijn voor de Operatie
Eis	VS2	9	Configuratiebeheer	8	Terugval organiseren	Opdrachtnemer stelt, vooraf aan de implementatie van elke wijziging, een terugvalscenario op, waarin opgenomen is onder welke condities wordt teruggestort en wie daartoe besluit.
Eis	VS2	9	Configuratiebeheer	9	Verifiëren van wijziging	Opdrachtnemer verifiëert direct na de implementatie van een wijziging, dat de wijziging is gelukt of dat het terugvalscenario wordt geactiveerd
Eis	VS2	9	Configuratiebeheer	10	Herstel	Opdrachtnemer zal noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebracht - als gevolg van incidenten met een bijzonder (urgent) karakter - achteraf alsnog de gebruikelijke procedures volgen en de configuratieinformatie actualiseren.
Eis	VS2	10	Testen	1	Relevant vooraf testen	Opdrachtnemer treft OTAP-voorzieningen om upgrades en patches op een relevante manier te testen vooraf aan implementatie in de operationele omgeving.
Eis	VS2	10	Testen	2	Integratietesten	Opdrachtnemer dient upgrades en patches te testen in de integrale testomgeving van Opdrachtgever vooraf aan implementatie in de operationele omgeving (OTAP).
Bindend informatief	VS-Algemeen	11	Fysieke toegang	1	Technische ruimte	Het Systeem wordt opgesteld in een technische ruimte van Opdrachtgever, voorzien van het EMMA-sluitsysteem.
Eis	VS1	11	Fysieke toegang	2	In publieke ruimte	Systeemkast die buiten (niet in technische ruimte) geplaatst worden, dienen te voldoen aan ...#nader te specificeren door MET
Eis	VS1	11	Fysieke toegang	3	Periferie	Opdrachtnemer voorziet in een door Opdrachtgever goedgekeurde cyberrisicoanalyse voor de fysieke en/of digitale bescherming van perifere systeemonderdelen die in de publieke ruimte staan (zoals camera, liften en OVCP-poortjes).
Eis	VS2	11	Fysieke toegang	4	Autorisatie	Opdrachtnemer dient erop toe te zien dat de toegang voor Personeel tot het Systeem uitsluitend op basis van het 'need to' principe plaatsvindt en daartoe bevoegd is
Eis	VS2	11	Fysieke toegang	5	Autorisatie	Opdrachtnemer dient de Opdrachtgever te bevragen over de wijze van fysieke en logische toegang voor Personeel tot het Systeem en mee te werken aan het werkvergunningensysteem van Opdrachtgever.
Eis	VS2	11	Fysieke toegang	6	EMMA-sluitsysteem	Opdrachtgever voorziet de systeem- en 19"-kasten van het EMMA-sluitsysteem uiterlijk vooraf aan de inbedrijfstelling. Voor die tijd mag Opdrachtnemer een eigen sluitsysteem hanteren. Het EMMA-sluitsysteem wordt geleverd door Opdrachtgever.
Eis	VS2	11	Fysieke toegang	7	Fysieke toegang	Opdrachtnemer dient gebruik te maken van de Procedure voor Fysieke toegang van Opdrachtgever.
Eis	VS2	11	Fysieke toegang	8	Werkvergunningen	De Opdrachtnemer dient voor alle werkzaamheden aan het Systeem Opdrachtgever vergunning aan te vragen bij het Vergunningenbureau van GVB en daartoe vooraf een Werkplan te overleggen
Eis	VS2	12	Online toegang	1	Beoogd gebruik	Opdrachtnemer zorgt ervoor dat Personeel de cybersecurity voorzieningen en maatregelen uitsluitend gebruiken zoals bedoeld.
Eis	VS2	12	Online toegang	2	IAA-gegevens	Opdrachtnemer heeft een procedure voor het toewijzen, vastleggen/opslaan en verspreiden van IAA-middelen, alsmede het onmiddellijk actualiseren daarvan en/of het innemen ervan bij vertrek, rol- of functiewisseling van medewerkers.
Eis	VS2	12	Online toegang	3	IAA-gegevens	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot het Systeem uit voorzorg de IAA te wijzigen.
Eis	VS2	12	Online toegang	4	Toegangsrechten	Opdrachtnemer dient de toegangsrechten van Personeel actueel te houden en bij overdracht aan Opdrachtgever en - in geval van een meerjarencontract - jaarlijks te actualiseren
Eis	VS2	12	Online toegang	5	Unieke ID's	Opdrachtnemer richt het Systeem zodanig in dat handelingen van Personeel te herleiden zijn tot unieke gebruikers-ID's
Eis	VS2	12	Online toegang	6	Vertrouwelijk	Opdrachtnemer zorgt er voor dat Personeel IAA-gegevens zeer-vertrouwelijk behandelt
Eis	VS2	12	Online toegang	7	Wachtwoorden	Opdrachtnemer zorgt ervoor dat Personeel en het Systeem alleen gebruik maken van sterke wachtwoorden. Zie document Wachtwoorden.
Eis	VS2	12	Online toegang	8	Logische toegangsbeheer	Opdrachtnemer dient erop toe te zien dat de toewijzing en het gebruik van IAA van beheerders beperkt dienen te blijven tot het noodzakelijke

Zie het tabblad Voorblad voor de status van dit document.

Eis-type	VS-type	Hoofdstuk-nummer	Hoofdstuk-titel	Paragraaf-nummer	Paragraaftitel	Paragraaftekst
Eis	VS2	12	Online toegang	9	Hardening	Opdrachtnemer zal alle remote toegang tot het Systeem blokkeren, tenzij het expliciet is toegestaan door Opdrachtgever
Eis	VS2	12	Online toegang	10	Auto log-out	Opdrachtnemer zorgt dat het Systeem - indien mogelijk - Personeel uitlogt na enkele minuten zonder interactie.
Eis	VS1	13	Hardening	1	Hardeningvoorschrift	Het Systeem is gehardend volgens het Hardeningvoorschrift, zie Referentie
Eis	VS2	13	Hardening	2	Hardeningsprocedure	Opdrachtnemer hanteert een Procedure voor het hardenen van het Systeem.
Eis	VS2	13	Hardening	3	Hardening in SC-plan	Opdrachtnemer beschrijft genomen de hardenings-voorzieningen en maatregelen in het Cybersecuritydossier
Eis	VS1	13	Hardening	4	Autorun voorkomen	Het Systeem voert een auto-run bij externe media niet uit.
Eis	VS2	13	Hardening	5	Reset wachtwoorden	Opdrachtnemer ziet er op toe dat alle standaard, default en fabrieks-wachtwoorden van het Systeem worden gereset. Zie document Wachtwoorden.
Eis	VS2	13	Hardening	6	Sterke wachtwoorden	Opdrachtnemer zorgt dat het Systeem alleen sterke wachtwoorden faciliteert.
Eis	VS1	13	Hardening	6	Geen koppeling met KA	Het Systeem mag geen directe verbinding met kantoornetwerken hebben.
Eis	VS2	13	Hardening	7	Testen op besmetting	Opdrachtnemer zal op basis van risico-analyses het Systeem op kwetsbaarheden en besmetting (periodiek) toetsen
Eis	VS2	13	Hardening	8	Bronverificatie	Opdrachtnemer dient bij het downloaden van Patches de broninternetsite te verifiëren door middel van een digitale handtekeningen en certificaat
Eis	VS2	13	Hardening	9	Testen van apparatuur	Opdrachtnemer toetst media en apparatuur op besmetting voordat die worden gekoppeld aan het Systeem
Eis	VS2	13	Hardening	10	Testen nieuwe software	Opdrachtnemer stelt de authenticiteit en integriteit van de software vast voorafgaand aan de implementatie op het Systeem.
Eis	VS2	13	Hardening	11	Actuele beveiligingspatches	Opdrachtnemer implementeert Patches zo snel mogelijk na bekendmaking, of vertraagd of versneld (urgentie) op basis van een risicoanalyse en goedkeuring van de Opdrachtgever.
Eis	VS2	13	Hardening	12	Antimalware	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware waarbij de anti-malware software en signature updates zodra bekend binnen een dag dienen plaats te vinden.
Eis	VS2	13	Hardening	13	Antimalware	Opdrachtnemer beschrijft de antimalware voorzieningen op in het Cybersecuritydossier
Eis	VS1	14	Koppelingen	1	Gebruik van NMA	Koppelingen met en tussen lokale netwerken, andere systemen of het internet vinden uitsluitend plaats via het NMA van MET
Eis	VS1	14	Koppelingen	2	NMA	Een koppeling met het Systeem en het NMA dient te voldoen aan de Aansluitvoorwaarden van het NMA.
Eis	VS1	14	Koppelingen	3	Toegang	Koppelingen van en naar het Systeem mogen uitsluitend met geregistreerde en beveiligde apparaten of systemen geschieden.
Eis	VS1	14	Koppelingen	4	Beperken	Opdrachtnemer dient het aantal netwerken en koppelingen met het Systeem te beperken tot strikt noodzakelijke
Eis	VS2	14	Koppelingen	5	Configuratiebeheer	Opdrachtnemer dient Koppelingen (remote toegangen, verbindingen en netwerken) en apparaten voor verbindingen als een configuratie-item actueel te beheren
Eis	VS2	14	Koppelingen	6	Hardening	Opdrachtnemer gebruikt nimmer onveilige protocollen, zoals en niet limitatief, FTP, Telnet, VNC en RDP
Eis	VS1	14	Koppelingen	7	2FA	Voor de remote Koppeling van en naar het Systeem wordt 2-factor- of biometrische authenticatie toegepast
Eis	VS1	14	Koppelingen	8	Internet	Een onbeveiligde koppeling met het Systeem en (via) een publiek netwerk - waaronder internet en e-mail - is verboden.
Eis	VS2	14	Koppelingen	9	Risicoanalyse	Opdrachtnemer dient voor elke type koppeling een risicoanalyse en afweging te maken en vast te leggen in het Cybersecuritydossier.
Eis	VS2	14	Koppelingen	10	Werkvergunning	Opdrachtnemer zorgt er voor dat remote (online) toegang alleen voor de geschatte duur van dat de werkzaamheden opengesteld is. De toegang wordt bewaakt en teruggezet bij afmelding van de call.
Eis	VS2	15	Backup	1	Periodiciteit	Opdrachtnemer maakt periodiek een backup van het Systeem met een frequentie en een bewaartermijn die past bij de dynamiek van en de operationele doelen van het Systeem.
Eis	VS2	15	Backup	2	Roll back	Opdrachtnemer dient back-ups te maken waarmee een volledige roll-back uitgevoerd kan worden naar de bedoelde configuratie en werkende operatie
Eis	VS2	15	Backup	3	Configuratie	Opdrachtnemer dient back-up kopieën van gegevens en programmatuur te registreren en actueel te houden als een configuratie-item.
Eis	VS2	15	Backup	4	Bewaartermijn	Opdrachtnemer dient back-ups bruikbaar actueel te houden.
Eis	VS2	15	Backup	5	Bewaarongeving	Opdrachtnemer beschermt back-ups en de ruimte waarin ze fysiek en online zijn opgeslagen volgens dezelfde normen die gelden voor de hoofdlocatie.
Eis	VS2	15	Backup	6	Scan op besmetting	Opdrachtnemer dient back-ups van het Systeem op te slaan op een locatie die zodanig afgeschermd is, dat geen schade aan de back-up kan worden aangericht als een cybercalamiteit zich voordoet op het productiesysteem.
Eis	VS2	15	Backup	7	Scan voor gebruik	Opdrachtnemer dient vast te stellen dat eerdere back-ups niet besmet zijn met malware die na de backup bekend zijn (gemaakt).
Eis	VS2	15	Backup	8	Systemimage	Opdrachtnemer dient vooraf en na iedere systeemwijziging systeemimages of back-ups te maken of aantoonbaar vast te stellen dan de eerder gemaakte back-ups actueel zijn.
Eis	VS2	16	Logging	1	Behandelen van logs	Opdrachtnemer dient logs/events van het Systeem te registreren, rapporteren, routeren, analyseren, kwantificeren en evalueren in relatie tot de operationele doelstellingen van het Systeem en de ernst van de events.
Eis	VS2	16	Logging	2	Bescherming	Opdrachtnemer ziet er op toe dat loggegevens in aparte bestand(en) worden weggeschreven; alleen toegankelijk voor geautoriseerd personeel; beschermd zijn tegen verlies of wijziging; minstens 1 jaar bewaard blijven; bewaard worden op aangeven van incident(feiten)onderzoekers.
Eis	VS1	16	Logging	3	Auto log	Logbestanden worden door het Systeem gegenereerd.
Eis	VS2	16	Logging	4	Afhandelen	Opdrachtnemer handelt meldingen, afkomstig van de integrale logging en monitoring van Opdrachtgever, af als een event/incident van het Systeem.
Eis	VS1	16	Logging	5	Opbouw log	Logbestanden bevatten minstens de volgende gegevens: de (type) gebeurtenis; de actor: een systeem-ID of een tot een natuurlijk persoon herleidbare user-ID; het systeem-ID waarop de gebeurtenis werd uitgevoerd; het resultaat van de gebeurtenis; de datum en het tijdstip van de gebeurtenis; een doorlopende unieke nummering per logregel; (optie) ID van werkstation; (optie) ID van fysieke en online locatie
Eis	VS1	16	Logging	6	IAA en sleutels	Logfiles bevatten nimmer IAA- en sleutelgegevens.
Eis	VS1	16	Logging	7	Integriteit	Het Systeem dient het overschrijven of verwijderen van logregels- en bestanden te loggen
Eis	VS1	16	Logging	8	Integriteit	Loginstellingen en logfiles zijn zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden
Eis	VS2	16	Logging	9	Integrale analyse en monitoring	Opdrachtnemer levert logbestanden van het Systeem eenmalig en/of periodiek aan, aan Opdrachtgever volgens een door Opdrachtgever vastgelegd formaat.
Eis	VS2	16	Logging	10	Beveiligingsmechanisme	Opdrachtnemer dient de ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die het Systeem genereert te activeren en te benutten voor registratie, rapportage en evaluatie van events en beveiligingsincidenten.
Eis	VS2	16	Logging	11	Toegang voor derden	De Opdrachtnemer dient toegang te geven aan een door Opdrachtgever aangewezen derde partij voor het plaatsen en gebruiken van sensoren (probes).
Eis	VS2	16	Logging	12	Specifieke logs	Opdrachtnemer zet specifieke loginstellingen en logsystemen in op verzoek van en in afstemming met Opdrachtgever.

Zie het tabblad Voorblad voor de status van dit document.

Eis-type	VS-type	Hoofdstuk-nummer	Hoofdstuk-titel	Paragraaf-nummer	Paragraaftitel	Paragraaftekst
Eis	VS2	16	Logging	13	Ontsluiten van logs	Opdrachtnemer levert logbestanden aan derden alleen na schriftelijke toestemming van Opdrachtgever.
Eis	VS2	17	Incident	1	Detectie	Opdrachtnemer hanteert Procedures om een cyberincident (op tijd) te detecteren, het effect op het Systeem en de impact op de Operatie (in samenwerking met de Opdrachtgever) te mitigeren en/of te herstellen.
Eis	VS2	17	Incident	2	Incidentmanager	Opdrachtnemer benoemt een cybersecurity incidentmanager met de bijbehorende verantwoordelijkheden en bevoegdheden.
Eis	VS2	17	Incident	3	Onregelmatigheden	Opdrachtnemer ziet er op toe dat afwijkingen in het wijzigingsproces vanuit cybersecurity worden beschouwd en - indien van toepassing - worden behandeld als een cybersecurityincident.
Eis	VS2	17	Incident	4	OTAP	Incidentafhandeling betreft de productieomgeving maar ook de test- en backupomgevingen.
Eis	VS2	17	Incident	5	Samenwerken	Opdrachtnemer dient samen te werken (en te oefenen) met Opdrachtgever en andere Opdrachtnemers voor het mitigeren, analyseren, veiligstellen en/of oplossen van incidenten (al of niet in een CSIRT-verband) tot en met het herstellen van het Systeem en de Operatie en eventueel de melding aan de betrokken autoriteiten, zoals de AP of het NCSC.
Eis	VS2	17	Incident	6	Samenwerken	Opdrachtnemer dient een procedure in te richten die aanhaakt en opvolging geeft aan geregistreerde cyberincidentmeldingen die worden aangedragen door de Opdrachtgever en/of nevenopdrachtnemers
Eis	VS2	18	Herstel	1	Hertstelprocedures	Opdrachtnemer hanteert procedures voor incidenten en het herstellen van het Systeem
Eis	VS2	18	Herstel	2	Dynamische gegevens	Opdrachtnemer dient bij Herstel rekening te houden met het terugzetten van de dynamische gegevens van het Systeem (systeemstatus).
Eis	VS2	18	Herstel	3	Samenwerken	Opdrachtnemer zorgt ervoor dat de procedures voor incidenten en herstel voor het Systeem passen op de integrale incident- en herstel (en calamiteitenplan) van opdrachtgever en nevenopdrachtnemers.
Eis	VS2	18	Herstel	4	Scan op besmetting	Opdrachtnemer dient periodiek vast te stellen dat back-ups niet gecompromiteerd (kunnen) zijn en dit vast te leggen in het Cybersecuritydossier
Eis	VS2	18	Herstel	5	Testen herstel	Opdrachtnemer dient herstelprocedures jaarlijks te controleren en testen en eventueel bij te stellen om te borgen dat ze doeltreffend zijn en binnen de gestelde tijd zoals beschreven in het Cybersecuritydossier van het Systeem kunnen worden uitgevoerd.
Eis	VS2	18	Herstel	6	Handbediende terugvalvoorziening	Opdrachtnemer dient een terugvalvoorziening te ontwerpen en te realiseren en af te stemmen met de Opdrachtgever, dat voorziet in een veilige (tijdelijke) handbediende Operatie, in geval het Systeem door een cyberaanval niet meer (correct) functioneert.
Eis	VS2	18	Herstel	7	Handbediende terugvalprocedures	Opdrachtnemer dient in samenhang met de terugvalvoorziening bedien- en beheerprocedures op te stellen en af te stemmen met de Opdrachtgever en t.b.v. de (toekomstige) Gebruiker en Beheerder, dat voorziet in een veilige (tijdelijke) handbediende Operatie.