Ministerie van Infrastructuur
en Waterstaat

BIACS

Basismaatregelen voor cybersecurity van IACS

Programma
Versterken
Cyberweerbaarheid
in de watersector

Colofon

	Bestuurskern DG Water en Bodem Den Haag
Datum	10 oktober 2022
Status	Definitief
Contactpersoon	J. Maes *Externe Medewerker* jessica.maes@minienw.nl
Versie	1.0
Opdrachtgever	
Auteur	Michael Theuerzeit (Hudson Cybertec)
Reviewers	Jeroen van den Berg (Min. IenW) Jessica Maes (Min. IenW) Daniel Keij (Gemeente Apeldoorn) Jeroen Gaiser (RWS) Kees van der Maarel (Min. Bzk.) Harold van Aalderen (Gemeente Rotterdam) Sylvia Bunte-Thelen (Min. Bzk.)

Inhoudsopgave

0 Inleiding

0.1 Aanleiding

Het belang van een goede digitale weerbaarheid is evident. Niet alleen in informatie verwerkende processen maar ook bij meet- en regelsystemen die voor de aansturing van industriële processen of gebouwbeheersystemen worden gebruikt. Omgevingen waarin deze systemen voorkomen worden ook wel Operationele Technologie (OT)[1] genoemd. Internationaal wordt de term IACS (Industrial Automation and Control Systems) veel gehanteerd.

In de wereld van informatiebeveiliging zijn standaarden zoals de ISO 27001/27002 (of BIO voor de overheid) veelal goed bekend. Voor het beveiligen van Operationele Technologie (OT) zijn deze kaders minder geschikt. Dit komt omdat de aspecten beschikbaarheid en integriteit van groter belang zijn dan bij informatieverwerkende processen. Er zijn internationaal ook kaders voor de beveiliging van OT, zoals het IEC 62443 normenkader. Naast de BIO, de Baseline Informatiebeveiliging Overheid, is de veelomvattende IEC 62443 door Rijkswaterstaat opgenomen in de CSIR, de Cyber Security Implementatie Richtlijn. De CSIR is vervolgens in nauwe samenwerking met het Waterschapshuis veralgemeniseerd tot een versie voor algemeen gebruik. Niet iedere organisatie die de CSIR wil gaan toepassen is echter al zo volwassen op gebied van cybersecurity dat zij deze volledig kan toepassen als best practice. Met deze “Basismaatregelen voor cybersecurity van IACS” worden organisaties op weg geholpen om de beveiliging van hun OT-systemen naar een hoger niveau te tillen. Doel is het document ook in de toekomst in lijn te houden met de CSIR. Daarmee dient dit document nu en in de toekomst tevens als opstap naar de uitgebreidere CSIR.

0.2 Doel van dit document

Dit document beschrijft de basismaatregelen voor cybersecurity van IACS-systemen in het OT domein. Het is geschreven vanuit het perspectief van de organisatie die eigenaar is van het primaire proces waar OT in worden gebruikt en daarmee verantwoordelijk voor de digitale weerbaarheid ervan. Organisaties krijgen hiermee een handreiking om de basisweerbaarheid van hun OT omgeving op orde te brengen. Daar waar wordt gerefereerd naar systemen, netwerken en voorzieningen, worden systemen, netwerken en voorzieningen binnen de OT omgeving van de organisatie zelf bedoeld. Het document is zo toegankelijk mogelijk opgebouwd. De basis maatregelen zijn gebaseerd op de CSIR en kennen dan ook een overeenkomstige structuur. De maatregelenset is gebaseerd op dezelfde tien thema’s uit de CSIR. Door de gekozen aanpak worden organisaties meegenomen bij het implementeren van de (basis-)maatregelen en ondertussen een start gemaakt met de implementatie van de uitgebreidere CSIR mocht dat in een later stadium gewenst zijn.

0.3 Relatie met andere documenten

0.3.1 ISO 27001/27002

De ISO 27001/27002 is een wereldwijd gebruikt normenkader voor informatiebeveiliging binnen de IT. De focus ligt op de vertrouwelijkheid van informatie. Beschikbaarheid van informatie en integriteit zijn hieraan ondergeschikt. De norm beschrijft hoe de digitale weerbaarheid kan worden gevat en onderhouden in een management systeem waarbij middels een PDCA-cyclus (Plan-Do-Check-Act) wordt gewerkt.
De ISO 27001/27002 vormen de basis voor, en kennen dezelfde opbouw als de BIO, waardoor verwijzingen in dit document naar specifieke BIO paragrafen ook in de meeste gevallen verwijzingen naar de ISO 27001/27001 betreffen. Aangezien de BIO is vormgegeven rondom de ISO 27001:2017, wordt deze versie hier ook gehanteerd.

0.3.2 BIO

De BIO is de Baseline Informatiebeveiliging Overheid. Het kader wordt verplicht gebruikt door rijksoverheid, gemeenten, provincies en waterschappen voor het managen hiervan de digitale weerbaarheid. De BIO is afgeleid van de ISO 27001/27002 en richt zich vooral op het aspect vertrouwelijkheid binnen informatiebeveiliging. Het kader is daarmee veel minder geschikt voor het beveiligen van Operationele Technologie (OT) omdat daar juist de aspecten beschikbaarheid en integriteit van belang zijn. Dit document maakt de koppeling naar verschillende controls uit de BIO. Hierdoor vertalen inspanningen volgend uit onderliggend kader zich naar de BIO.

[1] Binnen verschillende organisaties worden verschillende termen gebruikt voor het aanduiden van het OT domein. Termen die gebruikt worden zijn onder andere Proces Automatisering (PA), Industriële Automatisering & Controle Systemen (IACS) en Industriële Automatisering (IA). Waar dit document de term OT gebruikt, worden al deze systemen binnen dit domein bedoeld.

0.3.3 CSIR

De CSIR is de CyberSecurity Implementatie Richtlijn. Rijkswaterstaat heeft dit kader ontwikkeld voor het managen van de digitale weerbaarheid van haar objecten omdat de BIO (evenals diens voorganger de BIR) onvoldoende handvatten biedt voor de beveiligen van OT omgevingen. De CSIR put inspiratie uit de BIO en IEC 62443 en is opgebouwd rondom tien thema's voor cybersecurity. De CSIR gebruikt een controlset bestaande uit een algemene set van VSP's (vraagspecificatie proceseisen) en VSE's (vraagspecificatie systeemeisen) en beschrijft concrete cybersecuritymaatregelen op vier weerstandsniveaus. De CSIR is in samenwerking tussen Rijkswaterstaat en het Waterschapshuis veralgemeniseerd.
De BIACS is gepositioneerd als opstap naar de Cyber Security Implementatie Richtlijn (CSIR) en kent dan ook een overeenkomstige structuur. Echter, daar waar de CSIR uitgaat van vier weerstandsniveaus, voorziet deze handreiking in een gedeeltelijke invulling van weerstandsniveau 1. Door de beperkte set aan controls en maatregelen kunnen organisaties snel de eerste stappen zetten om de digitale weerbaarheid te vergroten en een eerste weerstandniveau bereiken. Waar de CSIR gebruik maakt van een controlset bestaande uit een algemene set van VSP's (vraagspecificatie proceseisen) en VSE's (vraagspecificatie systeemeisen), kent deze handreiking een beperkte set aan algemene controls en koppelt daarnaast specifieke controls aan de tien thema's.
In Appendix A is een mapping opgenomen van de controls uit dit document op de VSE's en VSP's uit de CSIR en een verwijzing naar de BIO. Zo wordt in 1 oogopslag duidelijk de overlap zit. Bij de maatregelen in hoofdstuk 2 is een referentie opgenomen naar de gebruikte nummering in de CSIR 3.0/3.4. Dit is gedaan om doorgroeimogelijkheden naar de CSIR vanuit onderliggend kader zo eenvoudig mogelijk te houden. Hierdoor komt het voor dat de nummering onderbroken wordt en er dus gaten in de nummering zitten.

0.3.4 IEC 62443

De IEC 62443 is een wereldwijd gebruikt normenkader voor cybersecurity van OT omgevingen. De verschillende normdelen zijn opgesteld door cybersecurity specialisten uit de OT. Eindgebruikers, leveranciers, system integratoren en consultancy partijen zijn betrokken bij de ontwikkeling en het onderhoud van het kader. De verschillende normdelen helpen alle partijen bij elke stap in de security lifecycle bij het op orde brengen en houden van de digitale weerbaarheid van OT omgevingen.
Maatregelen uit de IEC 62443 zijn opgenomen in de CSIR en daarmee ook in onderliggend document.

0.3.5 VRKI

De Verbeterde Risico Klasse Indeling is een instrument om het inbraakrisico van bedrijfspanden (en woningen) te bepalen.
Aan de hand daarvan wordt vastgesteld welke beveiligingsmaatregelen nodig zijn. Het document is met verzekeraars en beveiligingsexperts opgesteld en speelt een belangrijke rol bij het ontwerpen, opleveren en onderhouden van (gecertificeerde) beveiligingssystemen.
Dit document verwijst voor de fysieke beveiliging naar maatregelen zoals deze zijn opgenomen in de VRKI 2.0. Voor volledige transparantie en eenvoudige verwijzing zijn de afkortingen en codes zoals gebruikt in de VRKI waar van toepassing opgenomen bij de maatregelen voor fysieke beveiliging uit de BIACS.

0.4 Gebruikte terminologie

In dit document worden diverse termen gebruikt. Deze termen worden hieronder toegelicht:

Term	Toelichting
BIO	Baseline Informatiebeveiliging Overheid (zie: https://bio-overheid.nl)
CMDB	Configuration Management Database
CSIR	Cyber Security Implementatie Richtlijn: cybersecurity richtlijn voor OT, opgesteld en gebruikt door Rijkswaterstaat en diverse BAW partners. (zie: https://www.cert-wm.nl/csir)
CSMS	Cyber Security Management System
FAT	Factory Acceptance Test
IEC 62443	Cybersecuritynorm voor de Operationele Technologie (zie: https://www.nen.nl)
ISMS	Information Security Management System
ISO 27002	Cybersecurity norm voor informatiebeveiliging (zie: https://www.nen.nl)
ISO 27005	Norm voor Information Security Risk Management (zie: https://www.nen.nl)
Objecteigenaar	De afdeling of persoon binnen de organisatie die eindverantwoordelijk is voor de assets of beheerobjecten
Organisatie	De organisatie die eigenaar is van de assets of beheerobjecten
OT	Operationele Technologie
SAT	Site Acceptance Test
VRKI	Verbeterde Risico Klasse Indeling (zie: https://hetccv.nl/keurmerken/expert/inbraakbeveiliging/verbeterde-risicoklassenindeling-vrki/)
VSE	Vraagspecificatie systeemeisen
VSP	Vraagspecificatie proceseisen

0.5 Leeswijzer

Dit document beschrijft in hoofdstuk 0 het doel van dit document en hoe dit document zich verhoudt tot de CSIR.
De gedefinieerde algemene controls worden in hoofdstuk 1 toegelicht. De thema uitwerkingen komen aan bod in hoofdstuk 2. Voor elk van de tien behandelde thema's worden de van toepassing zijnde controls gedefinieerd en een set van concrete maatregelen gegeven.

De algemene en thema controls zijn een subset van de VSP's en VSE's uit de CSIR versie 3.0. De 10 thema's die worden uitgewerkt zijn:

1. Fysieke toegangsbeveiliging
2. Logische toegang
3. Beveiligingsincidenten en incident response plan
4. Netwerkkoppelingen en cryptografie
5. Bescherming tegen kwetsbaarheden
6. Logging en monitoring
7. Bewustwording en training
8. Gecontroleerd wijzigen
9. Beheer en onderhoud
10. Back-ups

Deze thema's sluiten volledig aan op de thema's uit de CSIR versie 3.0 en worden toegelicht in de betreffende themaparagrafen.

1 Algemene controls

De BIACS maakt gebruik van algemene controls en themacontrols behorende bij de tien thema's. De algemene controls zoals opgenomen in dit hoofdstuk beschrijven de algemene verantwoordelijkheden van de organisatie ten aanzien van de digitale weerbaarheid.

1.1 Hoofdcontrol

No.	Algemene hoofdcontrol
CTRL-01	Er dient voorkomen te worden dat gevaar of schade ontstaat door verstoring, uitval of misbruik van OT. Indien er toch schade ontstaat dient deze te worden hersteld.

1.2 Overige algemene controls

No.	Algemene proces control set
CTRL-02	(Beheer)processen dienen te worden ingericht en onderhouden conform de cybersecurity controls uit dit document.
CTRL-03	Aanvullend op de maatregelen in dit document kunnen de normen ISO 27002, IEC 62443 en CSIR worden geraadpleegd en opgevolgd.
CTRL-04	Voor de genomen cybersecurity controls en maatregelen dient elk jaar de opzet, bestaan en werking van de maatregelen middels een audit te worden aangetoond.
CTRL-05	Indien voorgeschreven cybersecurity controls en maatregelen niet worden doorgevoerd, dient dit gemotiveerd te worden vastgelegd (comply or explain) in een cybersecurity beveiligingsplan.
CTRL-06	De uitwerking van de cybersecurity controls voor de systemen dient vastgelegd te worden in een cybersecurity beveiligingsplan. Dit plan dient jaarlijks te worden geactualiseerd.
CTRL-07	Er dient een verantwoordelijke security functionaris te worden aangesteld die beschikt over relevante kwalificaties m.b.t. cybersecurity voor OT.
CTRL-08	Medewerkers die direct betrokken zijn bij cybersecurity van de OT omgeving of het primaire proces kunnen beïnvloeden dienen over een VOG te beschikken en geheimhouding in acht te nemen.
CTRL-09	Informatie binnen het OT domein (b.v. netwerktekeningen, IP tabellen) dient te worden geclassificeerd en volgens het toegekende classificatieniveau te worden behandeld. De afweging voor de classificatie gebeurt op basis van wettelijke eisen, waarde en gevoeligheid van informatie.
CTRL-10	Voorafgaand aan hergebruik of verwijdering van apparatuur dienen alle gegevens op de daarin aanwezige opslagmedia op betrouwbare wijze te worden verwijderd. Bij voorkeur gebeurt dit door een hiertoe gecertificeerde organisatie.
CTRL-11	Jaarlijks dient een risicoanalyse te worden uitgevoerd en worden opgevolgd met passende maatregelen. De eerste keer gebeurt dit vooraf aan het ontwerpproces van de OT systemen. Hiervoor kan de methodologie uit de ISO 27005 of gelijkwaardig worden gebruikt.
CTRL-12	De genomen maatregelen voor cybersecurity dienen jaarlijks te worden gemonitord, gemeten, geanalyseerd en geëvalueerd. Jaarlijks dienen er oefeningen plaats te vinden.
CTRL-13	De cybersecurity controls dienen te worden opgenomen in een security management systeem (b.v. ISMS of CSMS) van de organisatie.
CTRL-14	Het principe van gelaagde beveiliging dient te worden toegepast.
CTRL-15	OT systemen dienen gebruik te maken van invoer en uitvoer validatie om opzettelijk en onopzettelijk corrumperen van informatie te kunnen traceren.

2 Themauitwerkingen

2.1 Fysieke toegangsbeveiliging

Bij beveiliging van objecten en bijbehorende assets is fysieke beveiliging een eerste vereiste. Toegang van onbevoegden tot objecten en de OT infrastructuur dient te worden voorkomen. Hierbij wordt onderscheid gemaakt in maatregelen voor OT gerelateerde ruimten enerzijds en terreinen en gebouwen anderzijds. Voor de fysieke toegang is aansluiting gezocht bij de Verbeterde Risicoklassenindeling (VRKI 2.0[2]).

2.1.1 Controlset

No.	Controls fysieke toegangsbeveiliging
CTRL-16	De (beheer)processen voor de fysieke toegangsbeveiliging van alle terreinen, de gebouwen en OT gerelateerde ruimten (waaronder bedien- en technische ruimten) hierbinnen dienen te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-17	De fysieke toegangsbeveiliging van het terrein, de gebouwen en OT gerelateerde ruimten (waaronder bedien- en technische ruimten) hierbinnen dient te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-18	Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen.

2.1.2 Maatregelenset

2.1.2.1 *Maatregelen fysieke toegangsbeveiliging OT gerelateerde ruimten*

Toegangsbeheer		
No.	**Vereiste**	**CSIR 3.0 ref.**
1	Toegang tot OT gerelateerde ruimten is alleen mogelijk met (ten minste) een fysieke sleutel.	FR5

Toegangsproces		
No.	**Vereiste**	**CSIR 3.0 ref.**
2	Voor het verkrijgen van toegang tot OT gerelateerde ruimten zijn de binnen de organisatie geldende regels en processen van toepassing.	FR8

Organisatorisch		
No.	**Vereiste**	**CSIR 3.0 ref.**
3	Alle OT gerelateerde ruimten dienen bekend en gedocumenteerd te zijn.	-
4	Op OT gerelateerde ruimten zijn alle standaard organisatorische maatregelen uit de VRKI (zie ook O1 uit VRKI 2.0) van toepassing. Bijvoorbeeld: sleutelbeheer en -gebruik, sluitronde, beveiligingsverlichting, compartimenteren, huisregels, toegangscontrole, logboek.	FR9

Bouwkundig		
No.	**Vereiste**	**CSIR 3.0 ref.**
5	Bouwkundige maatregelen dienen te voldoen aan een prestatie-eis van 3 minuten inbraakwerendheid. (zie ook BK2 uit de VRKI 2.0)	FR11

[2] https://hetccv.nl/keurmerken/expert/inbraakbeveiliging/verbeterde-risicoklassenindeling-vrki/

Compartimentering		
No.	**Vereiste**	**CSIR 3.0 ref.**
6	Compartimenteringsmaatregelen dienen te voldoen aan een prestatie-eis van 3 minuten inbraakwerendheid. (zie ook CO2 uit de VRKI 2.0)	FR14
7	Er dienen meeneembeperkende maatregelen te zijn met prestatie-eis van 3 minuten diefstalvertraging. (zie ook ME2 uit de VRKI 2.0)	FR17

Elektronische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
8	Elektronische maatregelen dienen ten minste Grade 2 te zijn. (zie ook EL2 uit de VRKI 2.0)	FR20
9	Schil-detectie is ingericht en is in staat om nooduitgangen te detecteren. (zie ook SD1 uit de VRKI 2.0)	FR23

Alarmtransmissie		
No.	**Vereiste**	**CSIR 3.0 ref.**
10	Alarmtransmissie dient te voldoen aan alarmtransmissieniveau AT2. (zie ook AT2 uit de VRKI 2.0)	FR26

Reactie		
No.	**Vereiste**	**CSIR 3.0 ref.**
11	Inbraakalarmen dienen te worden doorgemeld aan een mobiele telefoon middels spraak of tekstbericht. Opvolging gebeurt middels persoonlijke verificatie door de objectverantwoordelijke of sleutelhouder. (zie ook RE1 uit de VRKI 2.0)	FR29

2.1.2.2 *Maatregelen fysieke toegangsbeveiliging terreinen en gebouwen*

Fysieke afscherming terrein		
No.	**Vereiste**	**CSIR 3.0 ref.**
12	Het afgebakend terrein dient te zijn voorzien van een Art. 461 bord (verboden toegang)	FTG1

Fysieke afscherming gebouw/compartiment		
No.	**Vereiste**	**CSIR 3.0 ref.**
13	Bouwkundige maatregelen en compartimentering dienen te voldoen aan een prestatie-eis van 3 minuten inbraakwerendheid (zie ook BK2 en CO2 uit de VRKI 2.0).	FTG6

Toegangsbeheer		
No.	**Vereiste**	**CSIR 3.0 ref.**
14	Er dient ten minste een mechanisch sluitplan te zijn ingericht.	FTG9

Organisatorisch		
No.	**Vereiste**	**CSIR 3.0 ref.**
15	Alle OT gerelateerde terreinen en gebouwen dienen bekend en gedocumenteerd te zijn.	-
16	Materialen mogen niet tegen gevels of hekken worden opgeslagen om inklimmen te voorkomen.	FTG28
17	Zwaar gereedschap dient te worden opgeslagen in een afgesloten kast of ruimte.	FTG32

2.2 Logische toegang

Naast het beperken van fysieke toegang, is het beperken van logische toegang noodzakelijk, zodat uitsluitend geautoriseerde personen toegang hebben tot de OT omgeving. Met logische toegang kunnen medewerkers op locatie of remote verbinding maken met de OT systemen.

2.2.1 Controlset

No.	Controls logische toegang
CTRL-19	De logische toegangsbeveiliging voor de OT omgeving dient te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-20	Er dient een formele en actuele procedure te zijn voor het registreren, verlenen, wijzigen en intrekken van fysieke en logische toegang tot OT.
CTRL-21	Alle gebruikers dienen zorgvuldig om te gaan met de aan hun toevertrouwde accounts en bijbehorende wachtwoorden. Complexiteit van de wachtwoorden dient daarbij in overeenstemming te zijn met de toegewezen mogelijkheden van het account.
CTRL-22	Toegang tot de OT omgeving op afstand dient via een formele procedure te worden aangevraagd en slechts goedgekeurd na het uitvoeren en documenteren van een risicoafweging.
CTRL-23	De OT omgeving dient logisch of fysiek te zijn gescheiden van de kantooromgeving.

2.2.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
18	De organisatie dient erop toe te zien dat: • medewerkers uitsluitend toegang krijgen tot OT en overige ondersteunende systemen wanneer dat noodzakelijk is voor hun werkzaamheden; • privileges van administrators en systeembeheerders beperkt dienen te blijven tot het strikt noodzakelijke; • alleen geautoriseerde personen logische en fysieke toegang hebben tot systemen, objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden; • disciplinaire maatregelen worden genomen bij misbruik van accounts en autorisaties.	LP2
19	De organisatie dient erop toe te zien dat: • alleen geauthentiseerde apparatuur toegang kan krijgen tot een vertrouwde zone waarbij alleen noodzakelijke privileges van software en apparatuur toegewezen en gebruikt worden; • privileges rolgebaseerd te koppelen zijn aan alle menselijke gebruikers; • gebruikersaccounts tijdelijk kunnen worden opgeschort.	LP3

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
20	De toegangsrechten van alle gebruikers worden minimaal eenmaal per halfjaar beoordeeld en geactualiseerd.	LP4
21	De lokale logische toegang voor medewerkers tot de OT omgeving dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager te worden aangevraagd en goedgekeurd. Hierbij wordt het volgende gedocumenteerd: details van de accounthouder, autoriserend manager, permissies behorende bij het account, geautoriseerde apparatuur.	LP5
22	Bij remote toegang voor beheer- en onderhoudsactiviteiten wordt uitsluitend gebruikt gemaakt van de speciaal hiervoor door de organisatie ingerichte dienst.	LP6
23	Medewerkers krijgen de beschikking over een wachtwoordkluis voor het beheren van hun accounts en wachtwoorden.	LP8
24	Beveiligingsmaatregelen mogen niet middels systeemhulpmiddelen, apparatuur of andere middelen worden omzeild.	LP9
25	Er is beschreven hoe de toewijzing en verspreiding van authenticatiemiddelen aan medewerkers, alsmede het innemen daarvan bij functiewisseling of vertrek (in-, door- en uitstroming) plaatsvindt. Daarbij is ook beschreven wat medewerkers moeten doen bij verlies, diefstal of beschadiging van deze middelen.	LP10
26	De toegang voor beheer en onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van het beheer en onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en afgesloten bij afmelding van het onderhoud, dan wel automatisch beëindigd na de vooraf ingestelde periode van openstelling.	LP12
27	Het overnemen van sessies op remote werkplekken vanuit een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	LP14

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
28	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA-gegevens in principe in versleutelde vorm worden uitgewisseld en opgeslagen.	LT1
29	De toegang tot OT en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.	LT2
30	Voor medewerkers en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.	LT3
31	(Standaard) wachtwoorden moeten door medewerkers bij het in gebruik nemen van de systemen gewijzigd kunnen worden .	LT7
32	Wanneer systemen alleen met generieke accounts kunnen werken moet dit worden gemotiveerd en vastgelegd waarbij de risico's in beeld gebracht worden.	LT8

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
33	De logische toegang dient als volgt te worden ingevuld: a. Lokale bediening – minimaal een user-ID en wachtwoord combinatie; b. Lokaal beheer en administrator accounts – 'two-factor' authenticatie ('bezit' plus 'kennis'); c. Remote toegang voor bediening, beheer en onderhoud - 'two-factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen.	LT12
34	Het gebruik van sterke wachtwoorden en vervangingsfrequentie dient instelbaar te zijn en te worden afgedwongen.	LT14
35	Bij het gebruik van een chipcardtoken of NFC-tokens voor toegang tot systemen wordt bij het verwijderen van het token het toegangsbeveiligingsslot automatisch geactiveerd.	LT16

2.3 Beveiligingsincidenten en incident response plan

De organisatie dient te zijn voorbereid op beveiligingsincidenten om te impact van het incident zo klein mogelijk te maken en zo snel als mogelijk terug te kunnen keren naar een veilige situatie. Indien een incident optreedt helpt een incident response plan bij het nemen van de juiste stappen om het incident in de kiem te smoren en terug te keren naar een veilige situatie.

2.3.1 Controlset

No.	Controls beveiligingsincidenten en incident response plan
CTRL-24	Incident response en recoveryplannen dienen te worden opgesteld en gevolgd voor de OT omgeving.
CTRL-25	Beveiligingsincidenten dienen direct te worden gemeld bij een hiervoor ingesteld centraal meldpunt. Hiervan dient een maandelijks rapportage te worden gemaakt en besproken.
CTRL-26	Bij een aanval, incident of calamiteit dienen OT systemen te kunnen schakelen naar een vooraf gedefinieerde veilige situatie (fail-safe design).

2.3.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
36	Beveiligingsincidenten en zwakke plekken in systemen of diensten worden volgens een geborgde procedure door alle medewerkers zo spoedig mogelijk gemeld bij het hiervoor aangestelde meldpunt.	IP1
37	Security incidenten worden via een geborgde procedure aangemeld, afgehandeld en geëscaleerd. Alle benoemde rolhouders kennen de inhoud van de procedure.	IP3
38	De verschillende incidentmanagementprocessen dienen op elkaar aan te sluiten.	IP4
39	De Incident Manager wordt ingeschakeld voor het afhandelen van urgente en niet-standaard security incidenten, zoals computervirusinfecties en aanvallen via publieke netwerken zoals internet.	IP5

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
40	Het operationeel incident response plan voor reactie op en afhandeling van incidenten en calamiteiten wordt jaarlijks geoefend en indien nodig aangepast. Daarbij wordt de noodbediening getest.	IP6
41	Het operationeel recovery plan voor recovery na incidenten of calamiteiten wordt jaarlijks geoefend en indien nodig aangepast.	IP7

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
42	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen te worden geactiveerd en benut voor registratie en rapportage van beveiligingsincidenten.	IT1
43	Het OT systeem dient bij een aanval naar een vooraf gedefinieerde veilige situatie te schakelen als normaal functioneren niet meer mogelijk is.	IT2
44	Het OT systeem dient na onderbreking of falen terug te kunnen keren naar een bekende veilige staat.	IT3
45	Het schakelen naar en van de geïnstalleerde noodstroomvoorziening voor het OT systeem en bediening mag geen invloed hebben op de beveiligingsstatus van het systeem.	IT4

2.4 Netwerkkoppelingen en cryptografie

OT netwerken zijn vaak gekoppeld aan andere omgevingen voor het uitwisselen van data, of het mogelijk maken van beheer en onderhoud op afstand. Het is van belang dat deze verbindingen beveiligd zijn zodat onbevoegden geen toegang kunnen krijgen tot de netwerken en de data.

2.4.1 Controlset

No.	Controls netwerkkoppelingen en cryptografie
CTRL-27	Bij het (tijdelijk) koppelen van beheer- en onderhoudsapparatuur aan de OT omgeving dient te worden voorkomen dat malware besmetting plaats kan vinden.
CTRL-28	Datanetwerkkoppelingen, inzet van cryptografie, draadloze verbindingen en lokale datanetwerkinrichting voor de OT omgeving dienen te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-29	Bij het uitvoeren van beheer- en onderhoudswerkzaamheden mogen geen rechtstreekse externe verbindingen (Internet, WiFi, GPRS, UMTS, inbelverbinding) worden gemaakt.
CTRL-30	Alle datanetwerkverbindingen van de OT systemen mogen uitsluitend verlopen via de centrale beveiligde voorzieningen.
CTRL-31	Dataverkeersstromen van productie, beheer en OTA dienen gesegmenteerd te zijn.

2.4.2 Maatregelenset

2.4.2.1 Maatregelen netwerkkoppelingen

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
46	Rechtstreekse (vaste of draadloze) verbindingen met de OT omgeving zijn niet toegestaan. Alle verbindingen lopen via de ingerichte beveiligde netwerkvoorzieningen en volgens de aansluitvoorwaarden van de organisatie. Remote toegang door derden dient daarbij altijd vooraf te worden aangevraagd volgens de hiervoor ingerichte procedures.	NP1
47	Alleen functioneel noodzakelijke koppelingen tussen de OT systemen en andere netwerken zijn toegestaan, mits de koppeling een passende vorm van beveiliging kent. Voor elke koppeling is een risicoanalyse en afweging gemaakt waaruit blijkt dat de koppeling geen onacceptabele risico's oplevert en de objectverantwoordelijke toestemming geeft.	NP4
48	Mobiele apparatuur en removable media van derden mogen binnen de OT omgeving uitsluitend worden ingezet na expliciete toestemming van de organisatie.	NP7
49	Alle datanetwerkkoppelingen dienen in kaart te worden gebracht, zodat altijd duidelijk is via welk netwerkpad een actor (uiteindelijk) een object zou kunnen binnendringen, beginnend vanuit het internet.	NP8
50	Actuele configuratiegegevens van het OT netwerk dienen beschikbaar te zijn.	NP9
Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
51	Verbinding tussen het kantoornetwerk en de OT omgeving (inclusief safety systemen, ondersteunende systemen en besloten lokale objectnetwerken) verlopen altijd via de beveiligde centrale voorzieningen van de organisatie.	NT1
52	Communicatie en functies van de safety systemen zijn afgeschermd van overige communicatie.	NT2
53	De integriteit van de gegevensoverdracht dient te worden geborgd door de gebruikte communicatiemethoden. Daarbij is ook aandacht voor eventuele fysieke en omgevingsinvloeden.	NT3
54	Alle informatie verwerkende systemen synchroniseren hun tijdklok met één centrale referentietijdbron binnen het netwerk.	NT4

2.4.2.2 Maatregelen cryptografie

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
55	Bij gebruik van cryptografie dienen door de organisatie vertrouwde certificaten te worden ingezet voor communicatie met (externe) netwerken buiten de eigen infrastructuur.	CP1
56	Bij gebruik van cryptografie dienen bij voorkeur eigen (interne) PKI certificaten te worden ingezet voor communicatie binnen de interne infrastructuur.	CP2

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
57	Het cryptografiebeleid omvat ten minste de volgende onderwerpen: • Wanneer wordt cryptografie ingezet; • Wie is verantwoordelijk voor de implementatie; • Wie is verantwoordelijk voor het sleutelbeheer; • Het gebruik, bescherming en levensduur van de cryptografische sleutels.	CP3
58	Bij gebruik van cryptografie dient te worden gekozen voor cryptografische toepassingen die voldoen aan passende standaarden.	CP4

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
59	Bij inzet van versleuteling (cryptografie) dient de gekozen versleuteling en de onderliggende algoritmes en instellingen uitsluitend de duiding “goed” te hebben zoals aangegeven in de meest actuele versie van het NCSC document “Richtlijnen voor Transport Layer Security”.	CT1
60	Het op afstand configureren van de OT systemen mag uitsluitend via beveiligde verbindingen plaatsvinden. Indien veilige communicatieprotocollen niet worden ondersteund dan dient vooraf goedkeuring verkregen te worden van de organisatie en een additioneel versleuteld kanaal worden toegepast (SSL, TLS, IPSEC etc.).	CT2

2.5 Bescherming tegen kwetsbaarheden

Management van kwetsbaarheden zorgt ervoor dat de daaraan verbonden risico’s worden gemitigeerd tot een voor de organisatie aanvaardbaar niveau. Het managen van kwetsbaarheden behelst anti-malware, systeem hardening en patch management.

2.5.1 Controlset

No.	Controls
CTRL-32	De OT systemen die niet door antimalware oplossingen worden beschermd dienen jaarlijks te worden gescand op malware middels antimalware op een USB, waarbij eventuele malware wordt verwijderd.
CTRL-33	Het patchen van OT systemen, de bescherming tegen malware en hardening van systemen dienen te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-34	Voedings- en communicatiekabels binnen de OT omgeving dienen te worden beschermd tegen interceptie, verstoring en schade.

2.5.2 Maatregelenset

2.5.2.1 *Maatregelen anti-malware*

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
61	Detectie en preventie van malware worden geborgd middels een procedure en bijbehorende voorzieningen.	AP1
62	Er is een recoveryplan met daarin opgenomen: • De voorzieningen voor back-up en herstel • Kopieën van gegevens en programmatuur • Benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware	AP3
63	Gegevensdragers, beheer- en onderhoudsapparatuur wordt gecontroleerd op en is aantoonbaar vrij van malware voordat deze wordt gekoppeld aan OT systemen of lokale objectdatanetwerken.	AP5

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
64	Antimalware voorzieningen worden correct geïnstalleerd en geconfigureerd. De juiste werking kan worden aangetoond met bijvoorbeeld EICAR.	AT1
65	Malware signatures, anti-malwaresoftware en bijbehorende herstelsoftware worden dagelijks geüpdatet.	AT3
66	De anti-malware voorzieningen mogen geen invloed hebben op de werking en functionaliteit van in gebruik zijnde OT systemen.	AT4

2.5.2.2 *Maatregelen hardening*

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
67	Er dient een geborgde procedure te zijn voor het hardenen van de OT omgeving.	HP1
68	Er wordt gebruik gemaakt van “good practice security baselines” voor veilige configuratie van hardware, software en netwerkapparatuur. Deze publiek beschikbare best practices uit de industrie worden opgesteld door leveranciers zoals bijvoorbeeld Microsoft[3] en andere stakeholders zoals bijvoorbeeld het NCSC.	HP2
69	Het weer inschakelen van uitgezette services en/of protocollen mag alleen door hiertoe geautoriseerd personeel worden uitgevoerd en wordt altijd gedocumenteerd.	HP4

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
70	Verwijderbare media (zoals b.v. USB-sticks, externe harde schijven) mag niet automatisch bestanden uitvoeren bij het aansluiten van het medium op een OT systeem. Auto-run moet zijn uitgeschakeld. Het uitvoeren van mobiele code is alleen toegestaan indien de code is geauthentiseerd en geautoriseerd. Het versturen van mobiele code van en naar OT systemen is geblokkeerd.	HT1

[3] https://www.microsoft.com/en-us/download/details.aspx?id=55319

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
71	De volgende hardening maatregelen zijn minimaal toegepast: • niet noodzakelijke datanetwerkservices zijn uitgeschakeld; • bekende kwetsbaarheden worden gepatcht; • alle poorten die niet nodig zijn worden geblokkeerd of uitgeschakeld; • alle default “access points” zijn verwijderd; • Alle standaard (fabrieks-) accounts zijn uitgeschakeld. Indien dit niet mogelijk is, is het wachtwoord gewijzigd naar een sterk wachtwoord dat voldoet aan de (volgens industrie best practice of beter) complexiteitseisen; • Security opties van leveranciers worden toegepast.	HT4
72	Het aanzetten van uitgeschakelde services en/of protocollen moet mogelijk blijven door uitsluitend hiertoe geautoriseerd personeel.	HT5

2.5.2.3 *Maatregelen patching*

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
73	Externe ICT-systemen mogen alleen gekoppeld worden aan de interne OT systemen als de externe systemen zijn voorzien van alle recente beveiligingsupdates en patches.	PP1
74	Patches worden alleen van betrouwbare bron afgenomen en voorafgaand aan installatie gecontroleerd op authenticiteit.	PP2
75	Indien patches niet kunnen worden uitgevoerd, dient een risicoafweging te worden gemaakt. Deze wordt samen met een mitigatievoorstel schriftelijk vastgelegd.	PP3
76	Er is een procedure voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokkenen zijn beschreven inclusief de van toepassing zijnde doorlooptijden.	PP5
77	Totdat implementatie van patches met NCSC classificatie Hoog/Hoog heeft plaats-gevonden worden passende tijdelijke mitigerende maatregelen getroffen.	PP6

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
78	De normale softwareprocessen op de OT systemen mogen geen zichtbaar structureel hinder ondervinden bij het uitvoeren van securityfuncties (b.v. netwerkscans, antimalware, patching).	PT1

2.6 Logging en monitoring

Het is van belang te weten wat er op het OT netwerk gebeurt. Het loggen van acties en monitoren van het netwerkverkeer maakt dit inzichtelijk. Hierdoor kunnen afwijkingen in het netwerkverkeer eerder worden opgemerkt en mogelijke indringers worden gestopt of configuratiefouten worden hersteld.

2.6.1 Controlset

No.	Controls
CTRL-35	Remote toegang en beheer op afstand voor OT dient te worden gemonitord en uitsluitend te verlopen via de centrale beveiligde voorzieningen.
CTRL-36	Het verzamelen, vastleggen en bewaren van gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen in logbestanden, het inrichten van een logserver daartoe en het analyseren van de beschikbare gegevens voor de OT omgeving dienen te voldoen aan de maatregelen uit dit hoofdstuk.

2.6.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
79	Er wordt op toegezien dat de volgende maatregelen worden uitgevoerd: a. de loggegevens worden voor een periode van tenminste 3 maanden weggeschreven en opgeslagen in een apart bestand, dat alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; b. de logbestanden van de OT omgeving, beveiliging en ondersteunende ICT-systemen en –netwerkelementen worden beschermd tegen verlies of wijziging; c. loggegevens die zijn gebruikt voor incidentonderzoeken worden op aparte media buiten de OT veiliggesteld; d. er is een overzicht van alle logbestanden die worden gegenereerd; e. een (onafhankelijke) interne audit procedure toetst ten minste elke 6 maanden op het ongewijzigd bestaan van de logbestanden; f. Indien loggegevens oneigenlijk worden gewijzigd, verwijderd of pogingen daartoe worden waargenomen, dient dit zo snel mogelijk te worden gemeld als beveiligingsincident.	MP1
80	Een operationeel proces voor de registratie en rapportage van netwerkstoringen binnen de OT omgeving is vastgelegd.	MP11
81	Ontdekte nieuwe dreigingen worden binnen de organisatie gedeeld met de verantwoordelijken voor de OT omgeving.	MP13
Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
82	De handelingen van personen en meldingen vanuit systemen en eventlogs worden vastgelegd in audit-logbestanden.	MT1
83	Ongeautoriseerde pogingen tot wijzigingen in software en opgeslagen gegevens dienen te worden gedetecteerd, gerapporteerd en voorkomen.	MT2

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
84	Logregels zijn voorzien van unieke en doorlopende nummering en bevatten minimaal de volgende gegevens: a. de gebeurtenis zelf; b. account of systeem dat de handeling uitvoert; c. component waarop de handeling werd uitgevoerd; d. het resultaat van de handeling; e. de datum en het tijdstip van de handeling.	MT4
85	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.	MT6
86	Het overschrijven of verwijderen van logregels en logbestanden wordt automatisch gelogd in een nieuw aangelegd logbestand.	MT7
87	De loginstellingen en logbestanden worden zodanig beschermd dat deze niet benaderd, gewijzigd of gewist kunnen worden door ongeautoriseerde personen of systemen.	MT8
88	Indien tijdens het verwerken van de loggegevens er fouten optreden, dient er een waarschuwing te worden gegeven aan een geautoriseerd persoon.	MT10
89	Binnen de OT omgeving wordt gebruik gemaakt van één referentietijdbron waarvan de integriteit is gevalideerd. Alle OT systemen synchroniseren met deze tijdbron.	MT19

2.7 Bewustwording en training

De mens wordt vaak gezien als zwakste schakel in cybersecurity. Door ervoor te zorgen dat de juiste maatregelen worden genomen op gebied van awareness en handelingsperspectief, worden medewerkers digitaal weerbaarder en kunnen incidenten worden herkend of zelfs voorkomen.

2.7.1 Controlset

No.	Controls
CTRL-37	Huisregels, gedragsregels en verantwoordelijkheden voor cybersecurity dienen in lijn met het beleid en procedures te worden opgesteld. Deze dienen bekend te zijn bij alle interne en externe medewerkers en waar relevant bij bezoekers. Het management is verantwoordelijk voor naleving hiervan.
CTRL-38	Interne en externe medewerkers dienen te handelen in overeenstemming met de maatregelen uit dit hoofdstuk.
CTRL-39	Bij beëindiging van een opdracht of contract met een externe partij dienen alle aan gebruikers van deze partij verstrekte bedrijfsmiddelen te worden ingenomen.

2.7.2 Maatregelenset

2.7.2.1 Maatregelen medewerkers

Maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
90	Medewerkers binnen de OT dienen periodiek awareness cursussen te volgen en hiernaar te handelen. De awareness trainingen besteden specifiek aandacht aan social engineering.	TMe1
91	Medewerkers binnen de OT zijn zich bewust van de voor hen van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weten dat gebruikers- en systeemactiviteiten worden gelogd.	TMe2
92	Medewerkers binnen de OT nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.	TMe3
93	Medewerkers binnen de OT doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management.	TMe4
94	Bij het constateren van een security incident dienen medewerkers binnen de OT dit direct als een security incident te melden bij de hiervoor verantwoordelijke. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het cybersecurity beleid of onregelmatigheid. Voorbeelden van security incidenten zijn: a. Uitval van diensten, apparatuur of voorzieningen, systeemstoringen of overbelasting als gevolg van cybersecurity inbreuken; b. menselijke fouten die leiden tot functionele verstoring of uitval van systemen; c. inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; d. Cybersecurity incidenten geïnitieerd vanuit de infrastructuur van opdrachtnemer en/of zijn netwerkproviders tot het netwerkdomein van opdrachtgever; e. inbreuk op de bediening en het beheer; f. ongeautoriseerde systeemwijzingen; g. niet-naleving van beleid of gedragsregels; h. detectie van malware; i. detectie van virus activiteit ; j. verlies of diefstal van ICT en OT bedrijfsmiddelen; k. oneigenlijk gebruik van bevoegdheden; l. vandalisme, moedwillige beschadiging.	TMe5
95	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de daarvoor verantwoordelijke.	TMe6
96	Medewerkers binnen de OT moeten bij het constateren van eventuele onregelmatigheden of onveilige situaties als gevolg van cybersecurity inbreuken, die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen, dan wel de schade beperken.	TMe7
97	Medewerkers binnen de OT gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangsmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen, en delen deze niet met collega's.	TMe8
98	Medewerkers binnen de OT creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.	TMe9

Maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
99	Medewerkers binnen de OT nemen de regels in acht voor de logische toegang tot OT systemen.	TMe10
100	Medewerkers binnen de OT koppelen geen mobiele apparatuur of removable media aan de OT omgeving. Uitgezonderd hiervan zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele malwarecontrole van apparatuur/media mogen doen.	TMe11
101	Voor medewerkers binnen de OT is toegang tot internet en het gebruik van email vanaf OT systemen strikt verboden.	TMe12
102	Medewerkers binnen de OT mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot OT systemen en netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.	TMe13
103	Medewerkers binnen de OT houden hun accountgegevens strikt geheim; zij gebruiken hun account en toegekende autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen of werken.	TMe14
104	Medewerkers binnen de OT dienen op OT systemen en netwerken de standaard/default/ fabrieks- accounts en/of wachtwoorden bij ingebruikname te verwijderen, uit te schakelen of ten minste te wijzigen.	TMe15
105	Bij het constateren van onregelmatigheden in de logische toegang tot OT systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de hiervoor verantwoordelijke.	TMe16
106	Alleen geautoriseerde medewerkers mogen systemen koppelen aan OT systemen en netwerken. Deze systemen dienen voorzien te zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur.	TMe17
107	Gegevensdragers worden altijd vooraf op malware gecontroleerd, voordat deze worden gekoppeld aan OT systemen en netwerken.	TMe18
108	Mobiele apparatuur en gegevensdragers mogen niet onbeheerd achtergelaten worden in openbare, vergader-, en conferentieruimten, in auto's of andere vervoermiddelen.	TMe19
109	Verlies of diefstal van mobiele apparatuur en gegevensdragers dienen zo spoedig mogelijk te worden gemeld als een security incident.	TMe20
110	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de hiervoor verantwoordelijke.	TMe21
111	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de hiervoor verantwoordelijke.	TMe22
112	Medewerkers binnen de OT zorgen ervoor dat onbeheerde OT systemen worden vergrendeld, ondersteund door een automatische vergrendeling na een vooraf in te stellen periode van inactiviteit.	TMe23
113	Medewerkers binnen de OT zijn zich bewust van de wijze waarop zij met vertrouwelijke informatie om te dienen te gaan, van het aanmaken en gebruiken van informatie tot vernietiging ervan.	TMe24

Maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
114	Medewerkers binnen de OT die beheer- en onderhoudswerkzaamheden uitvoeren aan OT systemen hebben een bewustwordingstraining voor cybersecurity gevolgd waarbinnen ook aandacht is besteed aan het vertrouwelijk omgaan met persoonsgegevens. Voor deze medewerkers geldt verder dat zij strikte geheimhouding in acht nemen en over een Verklaring Omtrent het Gedrag (VOG) beschikken zoals contractueel overeengekomen.	TMe25
115	Medewerkers mogen zonder voorafgaande goedkeuring geen apparatuur, informatie of software van de locatie meenemen.	TMe26
116	Het is voor gebruikers niet toegestaan zelf software te installeren.	TMe27

2.7.2.2 Maatregelen managers

Maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
117	Geschikte awareness training en bijscholing betreffende het cybersecuritybeleid, procedures en cybersecurityverantwoordelijkheden dient beschikbaar te worden gemaakt en gevolgd. Een ieder die zich bezig houdt met risicomanagement dient hier kennis van te hebben, dan wel hiervoor een specifieke aanvullende training te ontvangen.	TMa1
118	De organisatie draagt zorg voor en ziet erop toe dat: a. medewerkers binnen de OT aantoonbaar kennis hebben van cybersecurity; b. medewerkers binnen de OT de beschikbaar gestelde trainingen volgen en een actuele administratie hiervan aanwezig is; c. medewerkers binnen de OT de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de OT systemen; d. waar nodig geacht door de organisatie, werkzaamheden door gescreend personeel uitgevoerd. Bijvoorbeeld bij functies waarbij men directe invloed kan uitoefenen op de functionaliteit en werking van de OT omgeving; e. ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; f. medewerkers binnen de OT alle bedrijfsmiddelen en documentatie van de OT omgeving die ze in hun bezit hebben, retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; g. de toegangsrechten van medewerkers binnen de OT en de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, of na wijziging van de overeenkomst direct worden aangepast; h. calamiteitenplannen worden betrokken in de (awareness) trainingen en testactiviteiten.	TMa2
119	Cybersecurity wordt in de functioneringsgesprekken besproken met medewerkers.	TMa5
120	De organisatie dient bij het constateren van onregelmatigheden in de logische toegang tot OT systemen uit voorzorg altijd het betreffende account en wachtwoord te blokkeren en, na controle, eventueel zowel het account als het wachtwoord te laten wijzigen.	TMa6

2.8 Gecontroleerd wijzigen

Ook in OT omgevingen is het noodzakelijk dat wijzigingen worden doorgevoerd. Het is van belang hiervoor een gestructureerd proces te hebben ingericht. Hierdoor kunnen wijzigingen op de juiste wijze worden gemanaged zodat de digitale weerbaarheid geborgd blijft.

2.8.1 Controlset

No.	Controls
CTRL-40	Middels het wijzigingsproces dient assetinformatie voor de OT omgeving actueel te worden gehouden.
CTRL-41	De wijzigingsprocedures voor het doorvoeren van wijzigingen in de OT omgeving en de OTA (ontwikkel, test en acceptatie) omgeving dienen te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-42	De OTA (ontwikkel, test en acceptatie) omgeving dient gescheiden te zijn van de productieomgeving.

2.8.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
121	Een overzicht van alle apparatuur en diens instellingen wordt bijgehouden in een Configuration Management Database (CMDB). Deze CMDB dient actueel te worden gehouden.	WP1
122	Alle wijzigingen aan de OT omgeving worden conform de wijzigingsprocedure geregis-treerd. Ook Updates en patches dienen via de reguliere wijzigingsprocedure te verlopen.	WP2
123	Wijzigingen mogen alleen worden aangevraagd en uitgevoerd door geautoriseerde personen.	WP3
124	Jaarlijks worden de settings/configuraties van (ondersteunende) OT systemen in de CMDB vergeleken met de daadwerkelijke situatie. Afwijkingen in de CMDB worden gecorrigeerd.	WP5
125	Gegevensdragers en updates van software en firmware van technische systemen dienen eerst gescand te worden op malware voordat zij aan OT systemen worden gekoppeld en/ of geïnstalleerd.	WP7
126	Bij noodwijzigingen die buiten het reguliere wijzigingsproces om zijn doorgevoerd, worden achteraf alsnog de gebruikelijke procedures gevolgd en de CMDB administratie bijgewerkt.	WP9
127	Beveiligingsmaatregelen die tijdelijk zijn uitgeschakeld tijdens een wijziging worden weer geactiveerd alvorens de wijziging te sluiten.	WP11
128	Door te voeren wijzigingen en security patches worden vooraf in een testomgeving getest.	WP12

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
129	Ontwikkel-, test-, acceptatie en productieomgevingen (OTAP) zijn van elkaar gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. De volgende maatregelen worden als minimum doorgevoerd: a. Functionele scheiding van de ontwikkel, test, acceptatie en productieomgeving; b. De omgevingen zijn qua systemen en netwerk logisch of fysiek van elkaar gescheiden; c. Gebruikers dienen voor elke omgeving met andere gebruikersprofielen te werken; d. Voor de gebruikers is het altijd duidelijk in welke omgeving zij op dat moment werken; e. Elke omgeving dient conform de logrichtlijnen handelingen in logfiles vast te leggen die alleen toegankelijk is voor geautoriseerde personen; f. Er is een geborgd proces voor versiebeheer van de OTAP omgeving.	WT1

2.9 Beheer en onderhoud

Voor beheer en onderhoud van OT omgevingen is het van belang dat gestructureerd wordt gewerkt en dat acties herleidbaar en verklaarbaar zijn. Beheerpartijen dienen op de hoogte te zijn van wat hierin van hen wordt verwacht.

2.9.1 Controlset

No.	Controls
CTRL-43	Uitvoering van beheer en onderhoudswerkzaamheden voor de OT omgeving dient te voldoen aan de maatregelen uit dit hoofdstuk.
CTRL-44	Leveranciers en andere externe partijen dienen maximale hardening na te streven voor de apparatuur en delen van hun datanetwerk die nodig zijn voor het beheer en onderhoud van de OT omgeving.

2.9.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
130	Risico's en effectieve werking van de getroffen beheersmaatregelen worden geëvalueerd in het kader van life-cycle management.	OP1
131	In de beheer- en onderhoudscontracten met externe partijen wordt ervoor gezorgd dat, waar nodig: a. geheimhouding is opgenomen; b. training- en opleidingsvereisten alsmede overige benodigde certificeringen zijn beschreven; c. screening van personeel is geregeld (bijv. VOG); d. beschreven is dat de beveiligingshuisregels van de organisatie strikt in acht moeten worden genomen; e. een concrete escalatieprocedure is vastgelegd met betrekking tot incidentresponse met de leverancier (24*7) en dat deze bij alle betrokkenen bekend is; f. de procedures voor fysieke toegang tot objecten en ruimten, alsook de logische toegang tot systemen zijn vastgelegd; g. de registratie en rapportage van beveiligingsincidenten is geregeld; h. beschreven is dat handelingen van medewerkers en systemen worden gelogd en gemonitord; i. de procedure "Toegang Derden" van de organisatie voor de logische toegang tot netwerken en systemen moet worden gevolgd. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. j. beschreven is dat onderhoud en wijzigingen op OT systemen alleen uitgevoerd mogen worden vanaf systemen die zijn voorzien van de laatste security updates, patches en actuele viruscontroleprogrammatuur; k. beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van de organisatie verlopen; l. beschreven is dat wijzigingen conform het wijzigingsproces van de organisatie mogen worden uitgevoerd; m. beschreven is dat patchen strikt conform de patchrichtlijnen en doorlooptijden van de organisatie moeten worden uitgevoerd; n. beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; o. beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het netwerk van de organisatie strikt verboden is.	OP2
132	Er wordt zorg gedragen voor de beschikbaarheid, onderhoud en accuraat houden van (technische) beheerdocumentatie (waaronder fysieke en logische netwerktekeningen, verbindingen en configuratie documenten en een inventaris van alle apparatuur en software, inclusief versie- en serienummers), gebruikers- en/of installatiehandleidingen voor de OT systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.	OP4
133	Er is toezicht op de operationele uitvoering en naleving van: a. het doorvoeren van wijzigingen conform de wijzigingen procedure; b. de procedure voor fysieke toegang; c. de procedure voor logische toegang; d. patching, back-up procedure en bewaartermijnen; e. incidentmanagement, log- en incidentrapportages en de analyse daarvan.	OP6

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
134	Bedrijfsvertrouwelijke informatie is alleen op basis van het 'need-to-know' principe toegankelijk.	OP8
135	Geprinte exemplaren van documenten met classificatie bedrijfsinformatie (of gelijkwaardig) dienen in afgesloten kasten bewaard te worden. Bij digitale opslag in de eigen kantooromgeving is versleuteling niet verplicht.	OP10
136	Zowel actieve als passieve apparaten dienen te worden gecontroleerd op malware voordat deze worden verbonden met, of gebruikt in, de OT omgeving.	OP11
137	Het koppelen van beheer- en onderhoudsapparatuur aan OT systemen dient op veilige wijze te gebeuren.	OP12
138	Apparatuur dient correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	OP13

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
139	Voor de fysieke toegang van interne en externe medewerkers tot objecten en de ruimten hierbinnen, wordt gebruikt gemaakt van de producten en diensten van de organisatie.	OT1
140	Voor (remote) logische toegang van interne en externe medewerkers tot het netwerk en OT systemen wordt gebruikt gemaakt van de producten en diensten van de organisatie.	OT2
141	Gedurende FAT, SAT en onderhoud dient de werking van de cybersecurityfuncties in de systemen te kunnen worden aangetoond.	OT3
142	Het koppelen van beheer- en onderhoudsapparatuur aan OT systemen bij een object, dient op een veilige wijze te gebeuren.	OT5

2.10 Back-ups

Ondanks alle voorzorgmaatregelen kan het altijd voorkomen dat informatie corrupt raakt of verloren gaat . Het is daarom van belang dat betrouwbare back-ups beschikbaar zijn van de verschillende systemen.

2.10.1 Controlset

No.	Controls
CTRL-45	Het maken van back-ups van de OT omgeving volgens een te bepalen strategie, ondersteund door een ingericht back-up en recovery proces voor de OT omgeving, dient te voldoen aan de maatregelen uit dit hoofdstuk.

2.10.2 Maatregelenset

Organisatorische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
143	Systeemimages/back-ups worden gemaakt vooraf aan, en na iedere (functionele) systeemwijziging. De systeemimage/back-up van de laatste versie worden ten minste elk jaar vernieuwd. Met deze back-up moet men in staat zijn middels een volledige roll-back naar de werkende situatie terug te kunnen gaan. Indien back-ups gedurende de operationele fase van een object gemaakt moeten worden, dan mag dit het operationele proces niet verstoren.	BP1
144	De integriteit en beschikbaarheid van de laatste drie versies van de OT systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: a. Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevindt; b. Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; c. Back-ups worden bewaard tot het moment van uitdienstname van het betreffend systeem; d. In geval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.	BP2
145	Er zijn gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.	BP3

Technische maatregelen		
No.	**Vereiste**	**CSIR 3.0 ref.**
146	De benodigde voorzieningen voor het back-up en restoreproces worden in overleg ingericht.	BT1

Bijlage A Mapping controlset – VSP & VSE controls

Control	BIO verwijzing	Volgnummer VSP/VSE
CTRL-01	5.1.1	1 (VSP)
CTRL-02	5.1.1.1	2 (VSP)
CTRL-03	5.1.1.1	3 (VSP)
CTRL-04	5.1.1.1	4 (VSP)
CTRL-05	5.1.1.1	7 (VSP)
CTRL-06	5.1.1.1	9 (VSP)
CTRL-07	6.1.1	17 (VSP)
CTRL-08	7.1.1	21 (VSP)
CTRL-09	8.2.1	28 (VSP)
CTRL-10	11.2.7	42 (VSP)
CTRL-11	14.1.1.1	59 (VSP)
CTRL-12	15.2.1	69 (VSP)
CTRL-13	18.2.1.1	86 (VSP)
CTRL-14	5.1.1.1	92 (VSP)
CTRL-15	14.1.1	119 (VSE)
CTRL-16	11.1.2	39 (VSP)
CTRL-17	11.1.1	99 (VSE)
CTRL-18	8.1.3	26 (VSP)
CTRL-19	9.1.1	32 (VSP)
CTRL-20	9.2.1	34 (VSP)
CTRL-21	9.3.1	35 (VSE)
CTRL-22	9.4.2.2	37 (VSP)
CTRL-23	13.1.3	116 (VSE)

Control	BIO verwijzing	Volgnummer VSP/VSE
CTRL-24	5.1.1.1	15 (VSP)
CTRL-25	16.1.2.4	71 (VSP)
CTRL-26	16.1.5	127 (VSE)
CTRL-27	6.2.1	18 (VSP)
CTRL-28	13.1.1	54 VSP)
CTRL-29	13.1.2.3	55 (VSP)
CTRL-30	13.1.1	113 (VSE)
CTRL-31	13.1.3	117 (VSE)
CTRL-32	12.2.1	45 (VSP)
CTRL-33	12.6.1	51 (VSP)
CTRL-34	11.2.1, 11.2.3	103 (VSE)
CTRL-35	6.2.2	20 (VSP)
CTRL-36	12.4.1	108 (VSE)
CTRL-37	7.1.2	22 (VSP)
CTRL-38	7.2.1, 7.2.2	24 (VSP)
CTRL-39	8.1.4	27 (VSP)
CTRL-40	8.1.1	25 (VSP)
CTRL-41	12.1.2	44 (VSP)
CTRL-42	12.1.4	104 (VSE)
CTRL-43	14.1.1	58 (VSP)
CTRL-44	6.2.1.2	93 (VSE)
CTRL-45	12.3.1	107 (VSE)

Deze brochure is een uitgave van:

Ministerie van Infrastructuur en Waterstaat
Postbus 20901 | 2500 EX Den Haag
T 070 456 00 00

November 2022