ICT beveiligingseisen

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Verificatie methode(n):	Inkooponderdeel
1	Uniforme aanlevering incidentrapportages	VSP/VSE-eisen CSIR3.101	VSP03	De Opdrachtnemer dient de maandelijkse rapportage van security incidenten aan te leveren conform de bijlage CSR 21 "Uniform aanleveren van incidentrapportages".	BIO 2019: 16.1.2.4 en 16.1.3.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
2	Risicoanalyse	VSP/VSE-eisen CSIR3.100	VSP04	De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever. In de exploitatiefase dient de Opdrachtnemer ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken.	BIO 2019: 14.1.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
3	Aanstellen veranwoordelijke cybersecurity	VSP/VSE-eisen CSIR3.99	VSP05	De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de Werkzaamheden met betrekking tot cybersecurity.	BIO 2019: 6.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
4	Cybersecurity-eisen aan test- en onwikkelomgeving	VSP/VSE-eisen CSIR3.97	VSP07	De Opdrachtnemer dient de eisen ten aanzien van cybersecurity onverkort aan te houden bij de inrichting en onderhoud van een test- en ontwikkelomgeving.	BIO 2019: 14.2.5.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
5	Toepasselijkheid cybersecurity weerstandsniveau	VSP/VSE-eisen CSIR3.96	VSP08	De Opdrachtnemer dient voor alle beheerobjecten de van toepassing verklaarde maatregelen uit de Cybersecurity Implementatierichtlijn Objecten uit te voeren die behoren bij cybersecurity weerstandsniveau 1 tenzij er voor een beheerobject een ander cybersecurity weerstandsniveau is aangegeven. Noot: onder deze eis nog de volgende tabel: Beheerobject: xx – cybersecurity weerstandsniveau xx	BIO 2019: 5.1.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
6	Toepasselijkheid ISO27002 en IEC62443	VSP/VSE-eisen CSIR3.95	VSP09	Indien bijlage V "Cybersecurity Implementatierichtlijn Objecten" niet voorziet in cybersecuritymaatregelen voor de invulling van de cybersecurity eisen, dan dient de Opdrachtnemer de NEN-ISO/IEC 27002 (Code voor Informatiebeveiliging) en/of delen van de IEC 62443 standaards (Industrial Automation and Control Systems (IACS) Security) te volgen.	BIO 2019: 5.1.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
7	Toepasselijkheid Maategelen beheer en onderhoud	VSP/VSE-eisen CSIR3.94	VSP10	De Opdrachtnemer dient met betrekking tot het beheren en onderhouden van cybersecuritymaatregelen te handelen conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van bijlage V "Cybersecurity	BIO 2019: 14.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)

8	Transparantie bij afwijkingen	VSP/VSE-eisen CSIR3.93	VSP11	Indien de Opdrachtnemer tijdelijk niet aan cybersecurityeisen dreigt te voldoen, dan dient de Opdrachtnemer dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem en dient de Opdrachtnemer deze afwijkingenrapportage ter kennis te brengen van de Opdrachtgever en op te nemen in het	BIO 2019: 5.1.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
9	Handelingswijze bij inbreuken en verhoogde dreiging	VSP/VSE-eisen CSIR3.91	VSP13	De Opdrachtnemer dient met betrekking tot opvolging van cybersecurity inbreuken en/of verhoogde dreiging te handelen conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 13 "Handelswijze bij SOC incident melding en verhoogde dreiging" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".	BIO 2019: 16.1.5.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
10	Incident Response Plan	VSP/VSE-eisen CSIR3.90	VSP14	De Opdrachtnemer dient een proces met betrekking tot "incident response" te beschrijven (Incident Response Plan), conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" en conform de bijlage CSR 14 "Incident Response" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" een Incident Response Plan op te stellen.	BIO 2019: 16.1.5.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
11	Response op incidenten	VSP/VSE-eisen CSIR3.89	VSP15	De Opdrachtnemer dient de opgetreden cybersecurity incidenten te analyseren en maatregelen te treffen om herhaling te voorkomen. De Opdrachtnemer dient jaarlijks alle cybersecurity incidenten te analyseren en deze rapportage op te nemen in het cybersecurity dossier.	BIO 2019: 16.1.6.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
12	Problem Management	VSP/VSE-eisen CSIR3.88	VSP16	De Opdrachtnemer dient een proces inzake 'probleembeheer' te beschrijven zodanig dat security incidenten, waarvoor nog geen oplossing beschikbaar is, worden beheerst en zodanig dat op proactieve wijze nieuwe incidenten kunnen worden voorkomen en/of de	BIO 2019: 16.1.6.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
13	Verwerking van bewijsmateriaal	VSP/VSE-eisen CSIR3.87	VSP17	De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.	BIO 2019: 16.1.7.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
14	Logiscche toegangsbeveiliging IA-gerelateerde ruimten	VSP/VSE-eisen CSIR3.69	VSP35	De Opdrachtnemer dient met betrekking tot de logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten conform paragraaf 2.2 "Maatregelen Logische Toegang" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, cybersecuritymaatregelen te treffen.	BIO 2019: 9.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
15	Handelingswijze gebruik datanetwerk	VSP/VSE-eisen CSIR3.65	VSP39	De Opdrachtnemer dient met betrekking tot het datanetwerk te handelen conform paragraaf 2.4.1 "Netwerkkoppelingen" en conform de bijlage CSR 3 "Architectuur objectnetwerk" van bijlage V "Cybersecurity	BIO 2019: 13.1.3.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)

16	Securitymaatregelen bij datanetwerkkoppelingen	VSP/VSE-eisen CSIR3.64	VSP40	De Opdrachtnemer dient met betrekking tot datanetwerkkoppelingen cybersecuritymaatregelen te treffen conform paragraaf 2.4.1 "Netwerkkoppelingen" van bijlage V "Cybersecurity Implementatierichtlijn	BIO 2019: 13.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
17	Koppelen van randapparatuur	VSP/VSE-eisen CSIR3.62	VSP42	De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en IA van de Opdrachtgever de bijlage CSR 4 "Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" aan te houden voor bescherming tegen malware.	BIO 2019: 6.2.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
18	Hardening gekoppelde datanetwerkinfrastructuur	VSP/VSE-eisen CSIR3.61	VSP43	De Opdrachtnemer dient maximale hardening toe te passen voor zijn (rand)apparatuur en (delen van) zijn eigen datanetwerkinfrastructuur die ten behoeve van de Werkzaamheden gekoppeld zijn aan de datanetwerkinfrastructuur van de Opdrachtgever.	BIO 2019: 6.2.1.2.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
19	Toepassing Grip op SSD	VSP/VSE-eisen CSIR3.57	VSP47	De Opdrachtnemer dient voor het ontwikkelen en/of het onderhouden van software de gangbare principes en de voorgeschreven maatregelen uit het document "Grip op Secure Software Development (SSD) Beveiligingseisen voor (web)applicaties" van het Centrum Informatiebeveiliging en Privacybescherming (CIP) te	BIO 2019: 14.2.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
20	Escrow	VSP/VSE-eisen CSIR3.56	VSP48	De Opdrachtnemer dient voor het intellectueel eigendomsrecht, gebruiksrecht en Escrow van software voor ICT en IA de bijlage CSR 19 "Intellectueel Eigendom" van bijlage V "Cybersecurity Implementatierichtlijn Objecten" bij deze Vraagspecificatie Proces, te volgen. Opdrachtgever bepaalt op basis van een risico afweging tot inzet van Escrow.	BIO 2019: 18.1.2.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
21	Pentesten	VSP/VSE-eisen CSIR3.54	VSP50	De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever.	BIO 2019: 14.2.7, 18.2.3.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
22	Afwijkingsverzoek Patch management	VSP/VSE-eisen CSIR3.52	VSP52	Indien de Opdrachtnemer meent geen gebruik te maken van de mogelijkheid om te patchen, dan dient hij een gemotiveerd voorstel ter kennis te brengen van de Opdrachtgever.	BIO 2019: 12.6.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
23	Afhandeling bevindingen Opdrachtgever	VSP/VSE-eisen CSIR3.36	VSP68	De Opdrachtnemer dient negatieve bevindingen en tekortkomingen die door de Opdrachtgever zijn geconstateerd en gemeld aan de Opdrachtnemer, af te handelen op gelijke wijze als afwijkingen die door de Opdrachtnemer zijn geconstateerd.	BIO 2019: 18.2.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
24	Voorkomen van schade	VSP/VSE-eisen CSIR3.34	VSE01	De ICT en IA van het beheerobject dient zodanig te zijn ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.	BIO 2019: 5.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)

25	Gelaagde beveiliging beheerobject	VSP/VSE-eisen CSIR3.32	VSE03	De ICT en IA van het beheerobject dient zodanig te zijn gerealiseerd dat de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging is ingericht.	BIO 2019: 5.1.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
26	Hardening	VSP/VSE-eisen CSIR3.31	VSE04	Maximale hardening conform de maatregelen uit paragraaf 2.5.2 “Hardening” en bijlage CSR9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten] dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject.	BIO 2019: 6.2.1.2.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
27	Wachtwoordeisen beheerobject	VSP/VSE-eisen CSIR3.29	VSE06	Voor de ICT en IA van het beheerobject dienen de eisen en functionaliteit ten aanzien van wachtwoorden conform bijlage CSR 7 "Wachtwoorden" van de [Cybersecurity Implementatierichtlijn Objecten] gevolgd te worden.	BIO 2019: 9.3.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
28	Segmentering omgevingen beheerobject	VSP/VSE-eisen CSIR3.20	VSE15	De Ontwikkel-, Test-, Acceptatie-, Productie-, en Leeromgeving van het beheerobject dient gescheiden te zijn om het risico van onbevoegde toegang tot of veranderingen aan de productie omgeving te verlagen.	BIO 2019: 12.1.4.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
29	Datanetwerkkoppelingen beheerobject	VSP/VSE-eisen CSIR3.11	VSE24	De datanetwerkkoppelingen van het beheerobject dienen uitgevoerd te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten].	BIO 2019: 13.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
30	beveiligde verbindingen beheerobject	VSP/VSE-eisen CSIR3.10	VSE25	Alle datanetwerkverbindingen van het beheerobject dienen strikt en uitsluitend te verlopen via centrale beveiligde voorzieningen. Directe vaste of draadloze datanetwerkverbindingen met andere datanetwerken dan die van Opdrachtgever zijn strikt verboden.	BIO 2019: 13.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
31	Minimalisatie verbindingen beheerobject	VSP/VSE-eisen CSIR3.9	VSE26	Het aantal ICT en IA datanetwerkkoppelingen van het beheerobject met andere externe datanetwerken dient geminimaliseerd te zijn.	BIO 2019: 13.1.1.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
32	Segmentering datanetwerk beheerobject	VSP/VSE-eisen CSIR3.7	VSE28	Voor de ICT en IA van het beheerobject dient gebruik te zijn gemaakt van een gecompartimenteerde datanetwerk dat van de kantoorautomatisering is gescheiden. De scheiding kan fysiek of logisch zijn.	BIO 2019: 13.1.3.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
33	Segmentering datastromen omgevingen beheerobject	VSP/VSE-eisen CSIR3.6	VSE29	Voor de ICT en IA van het beheerobject dient segmentering van dataverkeersstromen toegepast te zijn voor Ontwikkel-, Test-, Acceptatie-, Productie-, Leer- en	BIO 2019: 13.1.3.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)
34	Inrichting datanetwerken beheerobject	VSP/VSE-eisen CSIR3.5	VSE30	De ICT en IA datanetwerken van het beheerobject dienen ingericht te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten].	BIO 2019: 13.1.3.	Overleg bewijsstukken en/of verklaring	Procesautomatisering (IACS-toepassingen)