Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

BIJLAGE C - Vraagspecificatie Security Eisen (VSS)

bij de EU aanbesteding

Meetboeien DEM inclusief Beheer en Onderhoud

Zaaknummer: 31207809

Colofon

Uitgegeven door	Ministerie van Infrastructuur en Waterstaat Rijkswaterstaat Centrale Informatievoorziening Derde Werelddreef 1 2622 HA Delft
Datum	7-7-2025
Status	Definitief
Versienummer	1.0

VERTROUWELIJKHEID
De informatie die in het kader van deze aanbesteding en de daaruit eventueel voortkomende opdrachten beschikbaar wordt gesteld, dan wel wordt vernomen, dient als vertrouwelijk te worden beschouwd.

Inhoud

1 Inleiding

Dit document Vraagspecificatie Security Eisen (hierna: VSS) bevat eisen op het gebied van security en informatiebeveiliging. De eisen zijn aanvullend op eisen die de Opdrachtnemer (hierna: OG) in de andere vraagspecificatiedocumenten geëist heeft. De eisen zijn opgesteld door het RWS Security Centre.

Het eerste hoofdstuk bevat eisen die voornamelijk gericht zijn op processen. Het tweede hoofdstuk bevat eisen die gericht zijn op ontwerp, bouw, test en het beheer & onderhoud van applicatie, systemen en producten.

De Opdrachtnemer (hierna: ON) dient aan alle eisen te voldoen, ongeacht in welk document deze vermeld zijn.

1.1 Nummering van contracteisen

De nummering van de eisen verwijst naar de overeenkomstige driepuntsnormen in het NEN document "ISO/IEC 27002:2013: IT Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging" en dient primair voor intern gebruik bij de OG. Omdat dit praktisch bleek, is in sommige gevallen van deze nummering afgeweken. Het gaat hier om de onderstaande afwijkingen:

1. In sommige gevallen is een eis in tweeën gesplitst; in dat geval zijn er een "a" een "b" achter de driepuntsnorm geplaatst om het onderscheid te kunnen maken;
2. In sommige gevallen zijn de driepuntsnormen onder één tweepuntsnorm samengevoegd tot één contracteis waarbij het derde cijfer in de driepuntsnorm-notatie is vervangen door een "x";
3. Eisen uit het CIP document "Cloud computing - Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)" waarvoor geen overeenkomstige eis bestaat binnen ISO/IEC 27002, zijn toegevoegd bij een corresponderende tweepuntsnorm, met als derde "cijfer" in de driepuntsnotatie "CC-n", waarbij "n" overeenkomt met het nummer van de norm uit het CIP document;
4. Eisen uit van het RWS Security Centre zelf waarvoor geen overeenkomstige eis bestaat binnen ISO/IEC 27002, zijn toegevoegd bij een corresponderende tweepuntsnorm, met als derde "cijfer" in de driepuntsnotatie "SC-*n*", waarbij "n" overeenkomt met het nummer op de lijst van SC-eisen.

Gedurende de looptijd van de overeenkomst zal in de communicatie tussen OG en ON verwezen kunnen worden naar de nummering indien een eis ter sprake komt.

2 Proceseisen informatiebeveiliging

2.1 Informatiebeveiligingsbeleid

Eisnummer	Omschrijving van de eis
5.1.1	ON borgt dat alle cybersecurity eisen uit dit VSS document worden ingevuld met beheersmaatregelen. Voor alle cybersecurity eisen van OG geldt het principe van comply or explain.
5.1.SC-01a	ON dient het deel van zijn informatievoorziening dat benodigd is voor de door de OG gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de OG geclassificeerde informatie en documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.
5.1.SC-01b	ON dient, daar waar OG niet verwijst naar specifieke beveiligingsrichtlijnen bij de te treffen maatregelen, de richtlijnen uit de meest recente versie van de NEN-ISO/IEC 27002 norm aan te houden.

2.2 Organiseren van informatiebeveiliging

Eisnummer	Omschrijving van de eis
6.1.1	ON dient voor ten minste alle processen genoemd in de Overeenkomst aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.
6.1.2	ON dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen, waarmee ook ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.
6.1.5	ON dient te beschikken over een operationeel geborgd projectbeheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.
6.2.1	ON dient een aantoonbaar operationeel geborgd proces te hebben voor het beveiligen en versleutelen van gegevens op mobiele apparatuur betrokken bij de Prestatie.

2.3 Veilig personeel

Eisnummer	Omschrijving van de eis
7.1.1	ON dient een aantoonbaar operationeel geborgd proces te hebben voor de screening van het Personeel dat werkzaamheden verricht: 1. op het gebied van ontwikkelen of herzien van ontwerptekeningen en/of -documenten; 2. ten behoeve van het ontwikkelen, testen, beheren, installeren, configureren en/of bedienen van programmatuur of apparatuur; 3. in bedienings- of technische ruimtes; 4. aan kabels en leidingen; 5. aan beveiligings- en veiligheidsdocumentatie en -instructies; 6. op locatie van de OG; en betrokken is bij de Prestatie middels ten minste een relevante Verklaring Omtrent Gedrag (VOG), waarbij gedurende de contractperiode een screening nooit ouder mag zijn dan 5 jaar. Hangende de aanvraag van een screening kan worden volstaan met een eigen verklaring van betreffende persoon gedurende een periode van maximaal zes weken gerekend vanaf de startdatum van deze persoon bij de Prestatie, welke niet verlengd kan worden.
7.2.2a	ON dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van OG ter sprake komen.
7.2.2b	ON dient aantoonbaar operationeel geborgd te hebben dat Personeel verantwoordelijk voor het testen van informatiesystemen betrokken bij de Prestatie, beschikken over actuele en gespecialiseerde kennis, ervaring en opleiding met betrekking tot het testen van de beveiliging hiervan.
7.3.1	ON dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel te communiceren dat: 1. deze van kracht blijven na beëindiging of wijziging van het dienstverband; 2. deze ten uitvoer moeten worden gebracht.

2.4 Beheer van bedrijfsmiddelen

Eisnummer	Omschrijving van de eis
8.1.1a	ON dient aantoonbaar operationeel geborgd te hebben dat van alle informatiesystemen betrokken bij de Prestatie een inventaris is opgesteld in een Informatie Technologie Configuratie Management Database (IT-CMDB), zodanig dat deze effectief kan worden gebruikt voor een effectief Configuration Management (CM) ITIL proces en dat deze CMDB actueel wordt gehouden.
8.1.1b	ON dient op verzoek van OG de gegevens vermeld in de Informatie Technologie Configuratie Management Database (IT-CMDB), van alle informatiesystemen betrokken bij de Prestatie, over te dragen.
8.1.SC-12	De ON dient alle door de OG beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, informatiesystemen en Industriële Automatisering) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.
8.2.1	Alle informatie betrokken bij de Prestatie dient te worden behandeld als RWS bedrijfsvertrouwelijke informatie, dient voorzien te zijn van dit vertrouwelijkheidskenmerk in zowel documenten als metadata. Als er persoonsgegevens en/of inloggegevens vermeld worden dient de informatie als RWS persoonsvertrouwelijk te worden behandeld.
8.3.x	ON dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media, het beheer van verwijderbare media en het onherstelbaar verwijderen van onnodige inhoud van herbruikbare media betrokken bij de Prestatie.

2.5 Toegangsbeveiliging

Eisnummer	Omschrijving van de eis
9.1.1	ON dient te zorgen voor een operationeel geborgde procedure voor het verschaffen van fysieke dan wel logische toegang tot informatieverwerkende faciliteiten, inclusief de uitgifte en inname van accounts en autorisaties, en een actuele registratie hiervan.
9.1.SC-02	Indien OG of derde partij verantwoordelijk is voor het verschaffen van de fysieke of logische toegang tot informatieverwerkende faciliteiten, dan dient ON zich te houden aan de door OG of derde partij gehanteerde toegangsprocedure.
9.1.SC-03	Indien ON of derde partij verantwoordelijk is voor het beheer en opslag van wachtwoorden van informatieverwerkende faciliteiten of voor deze informatieverwerking benodigde devices (als camera's, sensoren, etc.), dan dient de ON aan het einde van het contract alle door ON ingestelde/aangemaakte (admin)wachtwoorden over te dragen aan OG.

9.2.x	ON dient minimaal om het halve jaar zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces en zijn medewerking te verlenen voor de periodieke controle en schoning van de eindgebruikers accounts en rechten van OG.
9.4.5	ON dient aantoonbaar operationeel geborgd te hebben dat uitsluitend Personeel die daartoe specifiek bevoegd is, toegang heeft tot de Broncode van informatiesystemen betrokken bij de Prestatie.

2.6 Fysieke beveiliging en beveiliging van de omgeving

Eisnummer	Omschrijving van de eis
11.1.1	ON dient fysieke beveiligingszones te hebben gedefinieerd en in gebruik te hebben om gebieden te beschermen, die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, met betrekking tot de Prestatie.
11.1.5	ON dient aantoonbaar operationeel geborgde procedures te hebben voor het werken in beveiligde gebieden, zoals bedoeld in eis 11.1.1.
11.2.7	ON dient aantoonbaar te beschikken over een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de Prestatie.
11.2.8	ON dient aantoonbaar operationeel geborgde procedures te hebben voor de bescherming van onbeheerde informatiesystemen die betrokken zijn bij de Prestatie.

2.7 Beveiliging bedrijfsvoering

Eisnummer	Omschrijving van de eis
12.2.1	ON dient aantoonbaar operationeel geborgde processen te hebben voor bescherming tegen malware en virussen op informatiesystemen betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan preventie, detectie, communicatie en herstel.
12.3.1a	ON dient een aantoonbaar operationeel geborgd proces te hebben voor het minimaal dagelijks maken van back-ups van alle informatie en programmatuur in gebruik voor de Prestatie.
12.3.1b	ON dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar OG te communiceren over de uitkomst hiervan.

12.4.1	ON dient een aantoonbaar operationeel geborgd proces te hebben voor het voldoende periodiek beoordelen van logbestanden van informatiesystemen betrokken bij de Prestatie, waarbij het interval tussen twee beoordelingen nooit meer mag bedragen dan één maand.
12.4.3	ON dient een aantoonbaar operationeel geborgd proces te hebben voor het maandelijks beoordelen van activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie, welke zijn vastgelegd in logbestanden.
12.4.CC-21	ON dient logbestanden van informatiesystemen betrokken bij de Prestatie minimaal drie maanden (en bij een vermoed incident minimaal 3 jaar) beschikbaar te houden tenzij met OG een andere bewaartermijn is overeengekomen, en op verzoek deze logbestanden ter inzage te overhandigen aan OG.

2.8 Communicatiebeveiliging

Eisnummer	Omschrijving van de eis
13.1.1	ON dient, om informatie in informatiesystemen te beschermen, aantoonbaar operationeel geborgde processen te hebben voor beheer en beheersing van netwerken betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan onderstaande aspecten: 1. Management of network security; 2. Technical vulnerability management; 3. Identification and authentication; 4. Network audit logging and monitoring; 5. Intrusion detection and prevention; 6. Protection against malicious code; 7. Cryptographic based services; 8. Business continuity management.
13.1.SC-15	ON dient zorg te dragen dat het aantal data netwerkkoppelingen beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert. Voor elke koppeling is een risicoanalyse en afweging gemaakt.
13.1.SC-18	ON dient op verzoek van OG een actueel overzicht aan te leveren waarin alle datanetwerkkoppelingen worden weergegeven met bijbehorende securitymaatregelen.

2.9 Acquisitie, ontwikkeling en onderhoud van apparatuur en programmatuur

Eisnummer	Omschrijving van de eis
14.1.1	ON dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van informatiesystemen.

14.2.SC-06a	ON dient voor informatiesystemen betrokken bij de Prestatie binnen 60 dagen na kennisneming van kwetsbaarheden in het geval van programmatuur en binnen 6 maanden in het geval van apparatuur, kosteloos aanpassingen of patches vrij te geven (ten minste tot de door de Leverancier aangeduide End of Life (EOL) van dit informatiesysteem) met als doel deze kwetsbaarheden te verhelpen.
14.3.1	ON dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.

2.10 Leveranciersrelaties

Eisnummer	Omschrijving van de eis
15.1.3	De ON dient te borgen dat, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, bij de inkoop van diensten of producten van bedrijven de beveiligingseisen van OG door betrokkenen worden aangehouden.
15.1.SC-25	De ON dient, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, waarbij bij inkoop van diensten of producten vendorlock-in van een onderaannemer kan ontstaan en/of de nationale veiligheid in het geding kan worden gebracht, dit eerst voor te leggen aan OG.
15.2.1	OG heeft het recht om audit(s) uit te voeren waarin de eisen uit het contract tussen OG en ON worden getoetst op opzet, bestaan, en/of werking. Aan deze audit dient ON vrijwillig medewerking te verlenen.

2.11 Beheer van informatiebeveiligingsincidenten

Eisnummer	Omschrijving van de eis
16.1.x	ON dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van informatiebeveiligingsincidenten.

2.12 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Eisnummer	Omschrijving van de eis
17.1.2	ON dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties.

2.13 Naleving

Eisnummer	Omschrijving van de eis
18.1.3	ON dient aantoonbaar operationeel geborgde procedures te hebben voor het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave, van registraties op informatiesystemen betrokken bij de Prestatie, in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen.
18.1.SC-20	De ON dient maatregelen te treffen om documenten, zoals offertes, contracten, netwerkschema's, risicoanalyse uitwerkingen, kwetsbaarheidscans, penetratietestrapporten en accounts en wachtwoorden te beveiligen tegen spionage in de breedste zin des woords.
18.1.CC-09	Gegevens of programmatuur van OG, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van ON, is en blijft te allen tijde eigendom van OG. Indien gegevens door OG aan ON zijn verstrekt, mag Personeel dit alleen gebruiken voor het doel waarvoor dit is gebeurd.
18.1.CC-10	ON dient aantoonbaar operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van OG op apparatuur en alle back-up media van ON, na contractbeëindiging tussen beide partijen.
18.1.CC-12	Wanneer gegevens van OG zich bevinden op informatiesystemen van ON, dient bij contractbeëindiging tussen deze beide partijen, de ON assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar OG.
18.1.CC-14	Wanneer gegevens of programmatuur van OG zich bevinden op informatiesystemen van ON, dient ON aan te geven waar deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie[1].

[1] Momenteel zijn dit: Noorwegen, IJsland, bepaalde Kanaaleilanden, Argentinië, Canada, Zwitserland en de VS (met beperkingen).

18.1.SC-23	De ON dient bij inzet van certificaten voor publieke webdiensten de passende standaarden te hanteren conform de NCSC richtlijn ICT-beveiligingsrichtlijnen voor Transport Layer Security. Zie Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
18.2.1	ON dient tenminste jaarlijks een audit uit te voeren naar de opzet, bestaan en werking van de maatregelen op het gebied van de informatiebeveiliging gemeld in het contract met OG, en deze OG te rapporteren (als onderdeel van het Informatiebeveiliging Beveiligingsplan IV) over de bevindingen en voorgenomen verbetermaatregelen.
18.2.2	ON dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van beleidsregels, normen en andere eisen betreffende beveiliging, bij Personeel betrokken bij de Prestatie.
18.2.3	ON dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van technische beleidsregels, normen en andere eisen betreffende beveiliging bij informatiesystemen betrokken bij de Prestatie.
18.2.SC-09	ON dient een Informatiebeveiliging Beveiligingsplan uit te werken waarin de getroffen beheersmaatregelen zijn uitgewerkt en het Informatiebeveiliging Beveiligingsplan jaarlijks te actualiseren naar aanleiding van de periodieke beoordelingen van opzet, bestaan en werking van de beheersmaatregelen.
18.2.SC-10	ON dient in afstemming met OG het Informatiebeveiliging Beveiligingsplan op te stellen.

3 Eisen inzake informatiebeveiliging bij ontwerp, bouw, test en B&O

3.1 Organiseren van informatiebeveiliging

Eisnummer	Omschrijving van de eis
6.1.2	Informatiesystemen betrokken bij de Prestatie moeten zijn ingericht met een autorisatiemodel en voorzieningen waarmee ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.
6.2.1	Mobiele apparatuur in gebruik door Personeel moet gegevens gerelateerd aan de Prestatie versleuteld opslaan middels cryptografische toepassingen.

3.2 Toegangsbeveiliging

Eisnummer	Omschrijving van de eis
9.1.2	Informatiesystemen betrokken bij de Prestatie bevatten uitsluitend standaard voor programmatuur noodzakelijke functionele accounts of accounts die zijn aangeleverd door het vigerende autorisatieproces.
9.4.1	Accounts op informatiesystemen betrokken bij de Prestatie beschikken uitsluitend over toegangsrechten gekoppeld aan rollen toegekend via het vigerende autorisatieproces.
9.4.2	Informatiesystemen betrokken bij de Prestatie beschikken over een beveiligde inlogprocedure.
9.4.3	Informatiesystemen betrokken bij de Prestatie beschikken over wachtwoordbeheervoorzieningen die het gebruik van sterke wachtwoorden afdwingen.

3.3 Fysieke beveiliging en beveiliging van de omgeving

Eisnummer	Omschrijving van de eis
11.1.x	Informatieverwerkende faciliteiten op land betrokken bij de Prestatie zijn fysiek beveiligd middels sloten en een bewakings- en alarmsysteem.
11.2.x	Informatiesystemen op land betrokken bij de Prestatie zijn beschermd tegen verlies, schade, diefstal, compromittering of onderbreking.

3.4 Beveiliging bedrijfsvoering

Eisnummer	Omschrijving van de eis
12.1.4	ON dient ontwikkel-, test-, productie- en, indien besteld, educatieve omgevingen aantoonbaar gescheiden (logisch, dan wel fysiek) te hebben voor alle informatiesystemen betrokken bij de Prestatie. Scheiding houdt in dat al het noodzakelijke geregeld moet worden om interferentie tussen de omgevingen te voorkomen en dat de betrouwbaarheid van de productiesystemen gewaarborgd is. De acceptatie- en educatieve omgevingen dienen representatief te zijn voor de productieomgeving, zodanig dat de test- dan wel oefenresultaten het gedrag van de functionaliteit in de productieomgeving weerspiegelen.
12.2.1	Informatiesystemen betrokken bij de Prestatie zijn voorzien van detectieve en preventieve maatregelen tegen malware.
12.2.SC-13	De ON dient de informatiesystemen betrokken bij de Prestatie te hardenen door: • Niet noodzakelijke datanetwerkservices uit te zetten; • Het verwijderen (patchen) van bekende kwetsbaarheden; • Alle poorten die niet nodig zijn te deactiveren/blokkeren; • De default account uit te schakelen conform het wachtwoord policy; • Indien beschikbaar gebruik te maken van de security opties van de leveranciers; • De standaard hardeningsprofielen te volgen voor de gangbare platformen zie hiertoe bijv. de 'Security Benchmarks' van CIS: http://www.cisecurity.org/.
12.3.1	Informatiesystemen betrokken bij de Prestatie beschikken over voorzieningen om back-ups te kunnen maken van alle hier op aanwezige informatie en programmatuur.
12.4.x	Informatiesystemen betrokken bij de Prestatie leggen gebeurtenissen vast.

3.5 Communicatiebeveiliging

Eisnummer	Omschrijving van de eis
13.1.3	Groepen van informatiesystemen en gebruikers betrokken bij de Prestatie zijn op basis van functie, rol en/of classificatie in logische of fysieke netwerkdomeinen te scheiden volgens een zoneringsmodel.
13.2.3	Informatiesystemen betrokken bij de Prestatie die gebruik maken van elektronische berichten dienen hiervoor de vigerende versleuteling te gebruiken waarbij de gehanteerde onderliggende algoritmes en instellingen uitsluitend de duiding "goed" mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS). Zie Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

3.6 Acquisitie, ontwikkeling en onderhoud van apparatuur en programmatuur

Eisnummer	Omschrijving van de eis
14.1.2	Informatiesystemen betrokken bij de Prestatie die informatie uitwisselen via openbare netwerken moeten hiervoor te allen tijde versleutelde protocollen gebruiken waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding "goed" mogen hebben in de actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS). Zie Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
14.1.SC-03	Informatiesystemen betrokken bij de Prestatie zijn voor toegang op afstand en voor beheerdoeleinden niet anders te benaderen dan middels versleutelde protocollen, waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding "goed" mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS). Zie Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
14.2.8a	Informatiesystemen betrokken bij de Prestatie zijn aantoonbaar getest op kwetsbaarheden middels gangbare testmethodieken voordat deze in productie worden genomen.
14.2.8b	Alle bekende kwetsbaarheden op informatiesystemen betrokken bij de Prestatie zijn verholpen voordat deze informatiesystemen in productie worden genomen.
14.2.9a	Informatiesystemen betrokken bij de Prestatie dienen 'BIO compliancy' acceptatiechecks te hebben ondergaan op alle in dit overeenkomst vermelde systeemeisen voordat deze systemen in productie worden genomen.
14.2.9b	Informatiesystemen betrokken bij de Prestatie dienen niet in productie genomen te worden voordat alle bevindingen uit de 'BIO compliancy' acceptatiechecks zijn verholpen.

3.7 Naleving

Eisnummer	Omschrijving van de eis
18.1.5	Informatiesystemen betrokken bij de Prestatie beschermen informatie door middel van cryptografische maatregelen conform relevante overeenkomsten, wet- en regelgeving. Hierbij mogen uitsluitend algoritmes worden toegepast aangeduid als “goed” in de meest actuele versie van het NCSC document ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Zie Nationaal Cyber Security Center (NCSC), “ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)”, URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls