



RWS INFORMATIE

Informatiebeveiliging VSE

Informatiebeveiliging Vraagspecificatie-Eisen voor IV-contracten

| | |
|--------|------------------|
| Datum | 2 september 2019 |
| Status | definitief |

Colofon

| | |
|-----------------|---|
| Uitgegeven door | Security Centre, Rijkswaterstaat |
| Informatie | Marco Rijkschroeff / Turabi Yildirim/ Sahar Habib |
| Telefoon | |
| Fax | |
| Uitgevoerd door | Security Centre, Rijkswaterstaat |
| Opmaak | |
| Datum | 2 september 2019 |
| Status | definitief |
| Versienummer | 1.7 |

Inhoud

| | | |
|-----|---|----|
| 1 | Systemeisen informatiebeveiliging in IV-inkoopcontracten | 6 |
| 1.1 | Organiseren van informatiebeveiliging | 6 |
| 1.2 | Toegangsbeveiliging | 6 |
| 1.3 | Fysieke beveiliging en beveiliging van de omgeving | 6 |
| 1.4 | Beveiliging bedrijfsvoering | 6 |
| 1.5 | Communicatiebeveiliging | 7 |
| 1.6 | Acquisitie, ontwikkeling en onderhoud van apparatuur en programmatuur | 7 |
| 1.7 | Naleving | 8 |
| | Appendix A: Bronnen in contractteksten | 9 |
| | Appendix B: Nummering van contracteisen | 11 |

1 Systeemeisen informatiebeveiliging in IV-inkoopcontracten

OPMERKING: Dit document is een bijlage met de systeemeisen van het vastgestelde moederdocument "Informatiebeveiliging in standaard RWS IV-Contracteisen".

Verwijzingen naar externe documenten zijn vermeld als {n} en zijn terug te vinden in Appendix A. Verwijzingen naar externe richtlijnen zijn vermeld als IBR-n en zijn terug te vinden in het document Richtlijnen informatiebeveiliging bij RWS IV-contracteisen v1.0. Termen die beginnen met een hoofdletter zijn eigennamen en verwijzen naar specifieke betekenissen in de ARBIT en ARVODI contractteksten. Overige termen komen overeen met de definities genoemd in Nederlandstalige versie van NEN/IEC ISO 27000. Voor alle andere termen wordt verwezen naar de generieke betekenis, terug te vinden in het Van Dale Groot woordenboek van de Nederlandse taal. Achtergrondinformatie bij de gehanteerde nummering van eisen is terug te vinden in Appendix B.

1.1 Organiseren van informatiebeveiliging

- 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.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 6.2.1 Mobiele apparatuur in gebruik door Personeel moet gegevens gerelateerd aan de Prestatie versleuteld opslaan conform richtlijn IBR-1 *Beleid voor gegevensclassificatie* van Opdrachtgever middels cryptografische toepassingen waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding "goed" uit de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.

1.2 Toegangsbeveiliging

- 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 conform de richtlijn IBR-2 *Beleid voor logische toegangsbeveiliging* van Opdrachtgever.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 9.4.3 Informatiesystemen betrokken bij de Prestatie beschikken over wachtwoordbeheervoorzieningen die het gebruik van sterke wachtwoorden afdwingen die ten minste voldoen aan de richtlijn IBR-3 *Beleid voor wachtwoordgebruik* van Opdrachtgever.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

1.3 Fysieke beveiliging en beveiliging van de omgeving

- 11.1.x Informatieverwerkende faciliteiten betrokken bij de Prestatie zijn fysiek ten minste beveiligd volgens de richtlijn IBR-6 *Richtlijnen voor fysieke beveiliging* van Opdrachtgever.
- 11.2.x Informatiesystemen betrokken bij de Prestatie zijn beschermd tegen verlies, schade, diefstal, compromittering of onderbreking, waarbij ten minste de eisen worden geïmplementeerd uit de richtlijn IBR-6 *Richtlijnen voor fysieke beveiliging* van Opdrachtgever.

1.4 Beveiliging bedrijfsvoering

- 12.1.4 Opdrachtnemer 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 Opdrachtnemer dient de informatiesystemen betrokken bij de Prestatie te hardenen door:
- Niet noodzakelijke datanetwerkservices uit te zetten;
 - Het verwijderen (patches) 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. Indien informatiesystemen zich bevinden op de infrastructuur van de Opdrachtgever, moet dit kunnen gebeuren naar de centrale back-up voorziening van de Opdrachtgever.
- 12.4.x Informatiesystemen betrokken bij de Prestatie leggen gebeurtenissen vast waarbij ten minste wordt voldaan aan de eisen genoemd in de richtlijn *IBR-7 Richtlijnen voor logging* van de Opdrachtgever. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

1.5 Communicatiebeveiliging

- 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 netwerk domeinen te scheiden volgens een zoneringsmodel. Voor informatiesystemen geplaatst in de infrastructuur van Opdrachtgever, dient hiervoor het ontwerp (conform PSA) aangehouden te worden van Opdrachtgever.
- 13.2.3 Informatiesystemen betrokken bij de Prestatie die gebruik maken van elektronische berichten met daarin gegevens waarvan de vertrouwelijkheid en/of integriteit moet worden gewaarborgd, dienen hiervoor 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) {1}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

1.6 Acquisitie, ontwikkeling en onderhoud van apparatuur en programmatuur

- 14.1.1 In de programmatuur die deel uitmaakt van informatiesystemen betrokken bij de Prestatie zijn minimaal de maatregelen geïmplementeerd genoemd in het CIP document *Grip op SSD - Beveiligingseisen voor (web)applicaties* {3}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 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 meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 14.1.3 Informatiesystemen betrokken bij de Prestatie en die deel uitmaken van een keten, moeten afhankelijk van de classificatie van de uitgewisselde gegevens, te allen tijde de integriteit dan wel vertrouwelijkheid van deze gegevens waarborgen middels versleuteling, 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) {1}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de

- functionaliteit.
- 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) {1}.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 14.1.SC-26 Voor de ontwikkeling en onderhoud van mobiele applicaties dienen minimaal de maatregelen uit de *Handreiking Mobile App Ontwikkeling en Beheer voor de Rijksoverheid* {4} te worden toegepast.
- 14.1.SC-04a Informatiesystemen betrokken bij de Prestatie die geplaatst gaan worden in de infrastructuur van Opdrachtgever dienen conform de standaard aansluitvoorwaarden {5} van Opdrachtgever ingericht te zijn.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 14.1.SC-04b Informatiesystemen betrokken bij de Prestatie die geplaatst gaan worden in de infrastructuur van Opdrachtgever dienen gebruik te maken van de standaard netwerkdiensten {6} van Opdrachtgever.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- 14.2.8a Informatiesystemen betrokken bij de Prestatie zijn aantoonbaar getest op kwetsbaarheden middels gangbare testmethodieken voordat deze in productie worden genomen. In het geval van programmatuur omvat de gehanteerde testmethodiek ten minste de *OWASP Top-10* {7}.
- 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 een acceptatietest 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 voor dat alle bevindingen uit de acceptatietest zijn verholpen.

1.7 Naleving

- 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) {1}.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

Appendix A: Bronnen in contractteksten

In de contractteksten staan bronnen vermeld; het gaat hier om de volgende bronnen.

| Nummer | Bron |
|--------|--|
| { 1 } | 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 |
| { 2 } | Rijkswaterstaat IRN, "Afspraken en Procedures Netwerkdienstverlening: Netwerктоegang voor Derden", RWS Intranet URL: http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Lists/Veel%20gestelde%20vragen/DispForm.aspx?ID=49 |
| { 3 } | Centrum Informatiebeveiliging en Privacy (CIP), "Grip op SSD - Beveiligingseisen voor (web)applicaties", URL: https://www.cip-overheid.nl/category/producten/secure-software/ |
| { 4 } | Rijksoverheid: Handreiking Mobile App Ontwikkeling en Beheer voor de Rijksoverheid URL: https://www.noraonline.nl/wiki/Mobility |
| { 5 } | Rijkswaterstaat IRN, "RWS IV Aansluitvoorwaarden/RIVA", URL: Classificatie RWS Bedrijfsvertrouwelijk: https://werkwijzer.cf-prod.intranet.rws.nl/index.html Classificatie RWS Informatie: https://www.rijkswaterstaat.nl/zakelijk/zakendoen-met-rijkswaterstaat/werkwijzen/werkwijze-in-iv/index.aspx |
| { 6 } | Rijkswaterstaat IRN, "Aansluitvoorwaarden NNV Rijkswaterstaat" http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Algemeen_klanten/PDC%20en%20DAP/Forms/AllItems.aspx |
| { 7 } | Open Web Application Security Project (OWASP), "OWASP Top 10" https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project |
| { 8 } | BIO Handreiking Veilige afvoer van ICT-middelen https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Veilige-afvoer-van-ICT-middelen-v2.0.pdf |
| { 9 } | BIO Handreiking Mobile Device Management https://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/ |
| { 10 } | Richtlijnen informatiebeveiliging bij RWS IV-contracteisen v1.0 |
| { 11 } | BIO Handreiking Risicoanalysemethode https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/ |
| { 12 } | BIO Handreiking Penetratietesten https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten-v1-0/ |
| { 13 } | Handreiking Risicomanagement ISO-27005 |
| { 14 } | BIO Algemene handreiking continuïteitsbeheer https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/201903-Model-Continu%C3%AFteitsplan_v2.0.docx |
| { 15 } | Template Informatiebeveiliging Beveiligingsplan IV |
| IBR-1 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Beleid voor gegevensclassificatie" |
| IBR-2 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij |

| | |
|-------|--|
| | RWS IV-contracteisen", hoofdstuk "Beleid voor logische toegangsbeveiliging" |
| IBR-3 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Beleid voor wachtwoordgebruik" |
| IBR-4 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor beveiligen bij ontwikkelen" |
| IBR-5 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor informatiebeveiligingsincidenten" |
| IBR-6 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor fysieke beveiliging" |
| IBR-7 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor logging" |
| IBR-8 | Rijkswaterstaat Security Centre, "Richtlijnen informatiebeveiliging bij RWS IV-contracteisen", hoofdstuk "Richtlijnen voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS" |

Indien de contractteksten worden gebruikt door andere diensten dan Rijkswaterstaat kan ervoor gekozen worden om deze bronnen aan te passen naar eigen organisatie-specifieke bronnen. De bronnen die daadwerkelijk worden genoemd in een definitieve contracttekst dienen uiteraard als bijlage te worden meegestuurd met het contract (dat is niet noodzakelijk als de link publiekelijk toegankelijk is)!

Appendix B: Nummering van contracteisen

De nummering van de contracteisen 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 RWS gebruik. Omdat dit praktisch bleek is echter 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.