

Standaard Systeemeisen Cybersecurity

Uitgegeven door	RWS/CIV/SC
Vertrouwelijkheidsniveau	RWS Ongeclassificeerd
Datum	1 december 2015
Versie	1.0

Systeem topeis: Cybersecurity

Het systeem dient zodanig te worden ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.

Cybersecurity weerstandsniveau

De Infrastructuur RWS dient daar waar in deze overeenkomst direct of indirect verwezen wordt naar de specifieke implementatie richtlijnen uit de "Cybersecurity Implementatierichtlijn Objecten-RWS" te voldoen aan het hierna aangegeven cybersecurity weerstandsniveau. In alle gevallen geldt cybersecurity weerstandsniveau 1 behoudens en voor zover in de onderstaande tabel een ander cybersecurity weerstandsniveau is aangegeven voor de afzonderlijke objecten.

Noot: onder deze eis nog de volgende tabel:

Object: xx – cybersecurity weerstandsniveau xx

Gelaagde beveiliging

Het systeem dient de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging uitgevoerd te hebben.

Fysieke beveiliging

Het systeem dient fysieke beveiliging conform het Handboek Security Rijkswaterstaat uitgevoerd te hebben.

Fysieke toegangsbeveiliging

Het systeem dient de fysieke toegangsbeveiliging van IA gerelateerde ruimten (waaronder bedien- en technische ruimten) conform paragraaf 2.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten van Cybersecurity Implementatierichtlijn Objecten – RWS.

Plaatsing en bescherming van ICT en IA

Het systeem dient de ICT en IA tegen schade en storing beschermd te hebben.

Voedings- en telecommunicatiekabels

Het systeem dient voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden toegepast tegen aftapping of beschadiging beschermd te hebben.

Hardening

Het systeem dient gehardend te zijn conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van Cybersecurity Implementatierichtlijn Objecten – RWS.

Bescherming tegen malware

Het systeem dient beschermd te zijn tegen malware conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van Cybersecurity Implementatierichtlijn Objecten – RWS.

Back-ups

Het systeem dient de integriteit en beschikbaarheid van de ICT en IA te borgen door het maken van back-ups conform paragraaf 2.10 Maatregelen Back-ups van Cybersecurity Implementatierichtlijn Objecten – RWS.

Activiteiten in logbestanden

Het systeem dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vastgelegd te hebben in logbestanden conform paragraaf 2.6 Maatregelen Logging en Monitoring van Cybersecurity Implementatierichtlijn Objecten – RWS.

Compartimentering infrastructuur

Het systeem dient voor de IA gebruik te maken van een eigen gecompartmenteerde datanetwerk die van de kantoorautomatisering is afgescheiden. De scheiding kan fysiek of logisch zijn.

Segmentering van dataverkeersstromen

Het systeem dient segmentering van dataverkeersstromen voor productie, beheer en OTA toegepast te hebben binnen de lokale objectdatanetwerken voor de IA toepassingen.

Datanetwerkverbindingen

Het systeem dient alle datanetwerkverbindingen met het RWS datanetwerk strikt en uitsluitend gekoppeld te hebben via de centrale beveiligde voorzieningen en conform de [Nieuwe Netwerkvoorzieningen Verkeer en Waterstaat - Aansluitvoorwaarden].

Directe vaste of draadloze datanetwerkverbindingen van het Systeem met andere datanetwerken dan die van RWS zijn strikt verboden."

Minimalisatie datanetwerkkoppelingen

Het systeem dient het aantal datanetwerkkoppelingen tussen de ICT en IA met andere externe datanetwerken te minimaliseren conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van Cybersecurity Implementatierichtlijn Objecten – RWS.

Gebruik veilige communicatie protocollen

Het systeem dient indien het configureren van de ICT en IA-systemen van het Systeem op afstand plaatsvindt, dit over beveiligde verbindingen plaats te laten vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring door de Opdrachtgever het onveilige communicatieprotocol worden ingezet, mits er een additioneel encryptie kanaal wordt toegepast (SSL, TLS, IPSEC etc.).

Webapplicaties

Het systeem dient bij inzet van (web)applicaties de beveiliging van de in te zetten (web)applicaties opgebouwd te hebben conform het [Security kader voor (web)applicaties].

Validatie controles

Het systeem dient ICT en IA voorzien te hebben van invoer en uitvoer validatie controles om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.