

## DBFM Cybersecurity management eisen

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

### **Management topeis: Cybersecurity**

De Opdrachtnemer dient gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA te voorkomen.

### **Cybersecurity weerstandsniveau**

De Opdrachtnemer dient voor de Infrastructuur RWS de maatregelen uit de "Cybersecurity Implementatierichtlijn Objecten-RWS" behorende bij het hierna aangegeven cybersecurity weerstandsniveau uit te voeren. 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

### **Cybersecurity standaarden**

De Opdrachtnemer dient indien de "Cybersecurity Implementatierichtlijn Objecten-RWS" niet voorziet in maatregelen voor de invulling van de cybersecurity eisen, de NEN-ISO/IEC 27002 en de IEC 62443 te volgen.

### **Belegging verantwoordelijkheden**

De Opdrachtnemer dient voor cybersecurity de verantwoordelijkheden op de daartoe geëigende plaatsen binnen de projectorganisatie te beleggen.

### **Cybersecurity inbreuken en verhoogde dreiging**

Indien er sprake is van cybersecurity inbreuken of verhoogde dreiging, dient de Opdrachtnemer de richtlijn CS R03 Richtlijn voor handelwijze bij een hack, malwarebesmetting en verhoogde dreiging te volgen.

### **Evaluatie en verbetermaatregelen**

De Opdrachtnemer dient ten minste jaarlijks de maatregelen voor cybersecurity te monitoren en te meten.

### **Risicomanagement voor Cybersecurity**

De Opdrachtnemer dient ten aanzien van cybersecurity ten minste jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 of gelijkwaardig te maken.

### **Inventarisatie en registratie van Configuration Items**

De Opdrachtnemer dient alle Configuration Items (CI's) van de ICT en IA conform richtlijn CS R06 Richtlijn registratie CI items in een configuration management database te registreren in een Configuration Management Database (CMDB) en deze actueel te houden.

### **Beschikbaar stellen CMDB**

De Opdrachtnemer dient de informatie van de Configuration Items (CI's) zoals opgenomen in de Configuration Management Database (CMDB) beschikbaar te stellen aan andere beheer- en onderhoudsprocessen van Opdrachtgever.

### **Aanvaardbaar gebruik toegangsmiddelen**

De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.

### **Classificatie en beveiliging informatie**

De Opdrachtnemer dient voor de beveiliging van informatie van de Opdrachtgever en Documenten de door de Opdrachtgever aangegeven document-classificatie en bijbehorende beveiligingsmaatregelen aan te houden conform richtlijn CS R01 Richtlijn omgaan met vertrouwelijke informatie en documenten.

### **Bewustwording en scholing**

De Opdrachtnemer dient inzake bewustwording en training van (zelfstandige) Hulpverleners, voor zover relevant voor hun functie, maatregelen te treffen conform paragraaf 2.7 Maatregelen Bewustwording en Training van de Cybersecurity Implementatierichtlijn Objecten – RWS.

### **Verklaring Omtrent het Gedrag (VOG)**

De Opdrachtnemer dient de Werkzaamheden aan:

1. ontwerp- en constructietekeningen en constructieberekeningen en/of;
2. beveiligings- en veiligheidsdocumentatie en -instructies;

van:

- a. kunstwerken en/of;
- b. bediengebouwen en -ruimten en/of;
- c. dynamische verkeersmanagementsystemen en/of;
- d. ICT- en IA-systemen;
- e. kabels en leidingen;

dan wel de Werkzaamheden:

3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten;
4. aan ICT- en IA-systemen zelf;
5. aan kabels en leidingen;

door Hulpverleners te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en die over een Verklaring Omtrent het Gedrag (VOG) beschikken die gerelateerd is aan de beoogde Werkzaamheden. In afwachting van het resultaat van de aanvraag van een VOG kan gedurende een periode van maximaal zes weken na aanvang van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende Hulpverzoeker.

### **Documentatie bediening en beheer**

De Opdrachtnemer dient Documenten op te stellen en te onderhouden voor de bediening, het beheer, het onderhoud en de technische ondersteuning van ICT en IA.

### **Beveiliging documentatie**

De Opdrachtnemer dient de Documenten met betrekking tot ICT en IA te beveiligen tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.

### **Geborgde wijzigingsprocedure**

De Opdrachtnemer dient voor het doorvoeren van Wijzigingen aan ICT en/of IA een wijzigingsprocedure te hebben conform paragraaf 2.8 Maatregelen gecontroleerd wijzigen van de Cybersecurity Implementatierichtlijn Objecten - RWS.

### **Koppeling randapparatuur en bescherming tegen malware**

De Opdrachtnemer dient bij koppeling van randapparatuur aan de ICT en/of IA van de Opdrachtgever de richtlijn CS R02 Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT en IA systemen van RWS aan te houden voor bescherming tegen malware.

### **Back-ups en recovery proces**

De Opdrachtnemer dient conform "Cybersecurity Implementatierichtlijn Objecten – paragraaf 2.10 Maatregelen Back-ups" een proces in te richten voor back-ups en recovery. Het recovery proces dient jaarlijks te worden getest.

### **Beschikbaar houden van logbestanden**

De Opdrachtnemer dient de logbestanden van de ICT en IA beschikbaar te houden en op verzoek ter kennis te brengen van de Opdrachtgever.

### **Toegang geautoriseerden fysiek en logisch**

De Opdrachtnemer dient inzake logische toegang tot ICT en IA en de fysieke toegang tot ICT en IA gerelateerde ruimten maatregelen te treffen conform paragraaf 2.2 Maatregelen Logische Toegang van de cybersecurity Implementatierichtlijn Objecten – RWS.

### **Registratie toegang**

De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van:

- de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten;
- de door de Opdrachtnemer aan alle (zelfstandige) hulppersonen verstrekte accounts met bijbehorende autorisatie voor de logische toegang tot ICT en IA.

Indien de Opdrachtgever of derden de fysieke of logische toegangsprocedure regelen, dient de Opdrachtnemer deze toegangsprocedure te volgen.

### **Wachtwoordrichtlijn**

De Opdrachtnemer dient te handelen conform bijlage A Wachtwoord Richtlijn en bijlage B Factsheet Wachtwoorden van de Cybersecurity Implementatierichtlijn Objecten-RWS.

### **Datanetwerkkoppelingen**

De Opdrachtnemer dient inzake datanetwerkkoppelingen maatregelen te treffen conform paragraaf 2.4 Maatregelen Netwerkkoppelingen van de cybersecurity Implementatierichtlijn Objecten – RWS.

### **Remote access**

Indien de Opdrachtnemer toegang tot ICT en/of IA op afstand (remote access) wenst, dient de Opdrachtnemer deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van Opdrachtgever te laten verlopen.

### **Aanvraagformulier Netwerktogang voor Derden**

Indien de Opdrachtnemer toegang tot ICT en/of IA op afstand (remote access) wenst, dient de Opdrachtnemer een aanvraag in te dienen conform de procedure beschreven in "Aanvraagformulier Netwerktogang voor Derden" die de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.

### **Procedure melden en oplossen beveiligingsincidenten**

De Opdrachtnemer dient een centraal meldpunt in te stellen voor de registratie en het oplossen van beveiligingsincidenten conform paragraaf 2.3 Maatregelen Beveiligingsincidenten en incident Response Plan van Cybersecurity Implementatierichtlijn Objecten – RWS.

### **Rapportage beveiligingsincidenten**

De Opdrachtnemer dient direct aan de Opdrachtgever de beveiligingsincidenten te melden. De Opdrachtnemer dient maandelijks een rapportage te verstrekken van alle beveiligingsincidenten en van alle maatregelen die ter zake getroffen zijn.

### **Patchen**

De Opdrachtnemer dient voor het patchen van de ICT en IA-systemen te handelen conform paragraaf 2.5 Maatregelen bescherming tegen malware, hardening en patching van de Cybersecurity Implementatierichtlijn Objecten – RWS.

### **Risicoanalyse en implementatieadvies spoed patches**

Indien Opdrachtgever zelf melding maakt van spoed patches die niet kunnen wachten tot het eerst volgende patchmoment binnen het reguliere beheer en onderhoudsschema van Opdrachtnemer, dient Opdrachtnemer de Opdrachtgever per patch een implementatieadvies ter acceptatie voor te leggen. Daarbij gelden de volgende doorlooptijden:

- voor kritieke patches: maximaal 48 uur na melding door Opdrachtgever, gerekend vanaf de eerstvolgende werkdag;
- voor niet kritieke patches: maximaal twee maanden na melding door de Opdrachtgever.

De Opdrachtnemer dient de patches, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren.

### **Bewijsmateriaal verzamelen en bewaren**

De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen voor het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.

### **Continuïteit en herstel ICT en IA**

De Opdrachtnemer dient conform richtlijn CS R04 Richtlijn continuïteitsplan maatregelen te nemen en een continuïteitsplan te ontwikkelen om voorbereid te zijn op de gevolgen van omvangrijke storingen in de ICT en IA en spoedig herstel na storingen wordt bewerkstelligd.

### **Testen continuïteitsplannen**

De Opdrachtnemer dient minimaal jaarlijks de ontwikkelde continuïteitsplannen uit te voeren om te bewerkstelligen dat ze actueel en doeltreffend blijven.

### **Jaarlijkse beproevingen**

De Opdrachtnemer dient zijn medewerking te verlenen aan de beproevingen van de bediening, besturing en veiligheidsfuncties, die door de Opdrachtgever één keer per jaar worden uitgevoerd.

### **Cybersecurity Beveiligingsplan**

De Opdrachtnemer dient een Cybersecurity Beveiligingsplan op te stellen als uitwerking van de cybersecurity eisen waarbij de inhoud ten minste de onderdelen bevat uit:

1. paragraaf 2.9 Maatregelen Beheer en Onderhoud van de Cybersecurity Implementatierichtlijn Objecten – RWS;
2. de Template cybersecurity Beveiligingsplan.

### **Audit en rapportage beveiligingsmaatregelen**

De Opdrachtnemer dient minimaal een keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de rapportage ter kennis te brengen van de Opdrachtgever.

### **Wet bescherming persoonsgegevens**

De Opdrachtnemer dient in het kader van de Wet bescherming persoonsgegevens de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen.

### **Wbp bewerkersovereenkomst**

Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt dient de Opdrachtnemer een bewerkersovereenkomst af te sluiten met de Opdrachtgever conform het sjabloon "RWS bewerkersovereenkomst" die de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.

### **Videocamera's en opslag videobeelden**

Indien de Opdrachtnemer beheer en onderhoudswerkzaamheden uitvoert aan videocamera's en/of systemen waarin camerabeelden zijn opgeslagen, dient de Opdrachtnemer de richtlijn CS R05 Richtlijn camera's en omgang met camerabeelden van de verkeersregistratiesystemen te volgen.

### **Beveiliging spionage**

De Opdrachtnemer dient op basis van risicoanalyse maatregelen tegen spionage te nemen zodanig dat de Documenten met betrekking tot ICT en IA, waaronder documentatie, offertes, contracten, netwerkschema's, modellen, tekeningen en berekeningen, zijn beveiligd tegen verlies en ongeautoriseerde kennisname en ongeautoriseerde wijziging.

### **Beveiliging van de Informatievoorziening**

De Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.