

## **RWS voorwaarden Externe koppelingen**

Datum	8 december 2011
Status	v1.02



## **RWS voorwaarden Externe koppelingen**

Datum	8 december 2011
Status	v1.02
Auteurs	A.P.F. Poeltuyn E. van Vliet

## Inhoud

- 1        Inleiding 5**
- 2        Voorwaarden 6**

## 1 Inleiding

Het RWS netwerk levert de communicatie en transmissie dienstverlening ten behoeve van Rijkswaterstaat informatie systemen.

Voor het toegang krijgen door derde partijen tot netwerkinfrastructuren en de daarop aangesloten informatie systemen inclusief objecten met industriële automatisering en beheersystemen zijn voorwaarden opgesteld. Dit om de beveiliging van het RWS netwerk en de daarop aangesloten systemen en informatie te kunnen waarborgen.

Deze voorwaarden gelden voor het aansluiten van infrastructuren en systemen van Derden en het gebruiken van informatie systemen.

Indien koppelingen met onderaannemers van de Derde partij nodig zijn dan gelden tevens deze voorwaarden voor die koppelingen en activiteiten.

## 2 Voorwaarden

- 1 Een rijksoverheidsinstelling hanteert de VIR2007 en de daarbij behorende departementale Baselines Beveiliging voordat aansluiting wordt geautoriseerd.
- 2 Een niet-rijksoverheidsinstelling heeft een beveiligingsbeleid gebaseerd op de Code voor Informatiebeveiliging of een hieraan gelijkwaardige norm (zoals NEN-ISO/IEC 27001:2005) voordat aansluiting wordt geautoriseerd.
- 3 Gebruik van de ICT-faciliteiten die strijdig zijn met de doelstelling en het imago van Rijkswaterstaat, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten Rijkswaterstaat is niet toegestaan. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en /of toepassingen die strijdig zijn met de wet of als onethisch te karakteriseren zijn.
- 4 Elke Derde Partij dient te voldoen aan de hiervoor liggende koppelvoorwaarden. Bij overtreding van deze voorwaarden of het niet kunnen of willen voldoen kan er door Rijkswaterstaat worden besloten tot afsluiting van de dienst voor de Derde Partij. In uitzonderlijke gevallen wordt dit doorgevoerd zonder enige communicatie vooraf.
- 5 De Derde Partij moet op verzoek van Rijkswaterstaat kunnen aantonen welke maatregelen men heeft getroffen om aan de hiervoor liggende voorwaarden te voldoen.
- 6 Het is niet toegestaan om elektronische informatie- en communicatiemiddelen zodanig te gebruiken dat de systeem-, informatie-, applicatie- en/of netwerkbeveiliging (opzettelijk) worden aangetast.
- 7 Diensten van Derde partijen mogen niet leiden tot een aantasting van de betrouwbaarheid (beschikbaarheid, integriteit of vertrouwelijkheid) van de ICT-voorzieningen en Informatie van Rijkswaterstaat en/of de andere aan het Rijkswaterstaat netwerk aangesloten (Derde) partijen.
- 8 De Derde Partij dient onmiddellijk de beveiligingsfunctionaris van Rijkswaterstaat te informeren indien er sprake is, of een redelijk vermoeden bestaat van ongevoegde toegang tot computers en/of netwerken van de Derde Partij. De Derde partij dient zelf een aanspreekpunt voor beveiligingszaken aan te wijzen en te communiceren.
- 9 Het is de Derde Partij niet toegestaan om rechten of verplichtingen over te dragen zonder voorafgaande schriftelijke toestemming van Rijkswaterstaat.

- 10 Rijkswaterstaat en de Derde Partij nemen de noodzakelijke veiligheidsmaatregelen op hun eigen informatiesystemen, waaronder inbegrepen de veiligheidsmaatregelen zoals in dit document beschreven, om elkaars informatiesystemen te behoeden tegen verlies van betrouwbaarheid.
- 11 De Derde Partij heeft op haar informatiesystemen maatregelen genomen om overlast door malware (o.a. virus, worm en trojan) voor Rijkswaterstaat te voorkomen.
- 12 Koppeling met de infrastructuur van Rijkswaterstaat door een Derde Partij vindt plaats na toestemming op basis van een (Underpinning) Contract en/of een schriftelijke samenwerkingsovereenkomst.
- 13 Koppelingen tussen verschillende informatiesystemen en netwerken vereist tussen de betrokkenen schriftelijke afspraken over het vereiste beveiligingsniveau van de informatie en de vereiste wederzijdse beveiligingsmaatregelen en aansprakelijkheid.
- 14 Beide partijen moeten het gebruik van de koppeling beperken tot de activiteiten en functionaliteiten die zijn overeengekomen en de koppeling mag niet voor andere doeleinden worden gebruikt.
- 15 De TCP/IP-protocolsuite is de communicatie standaard.
- 16 De toegang van de bronsystemen naar doelsystemen zal gelimiteerd worden tot de IP protocollen inclusief poorten en adressen die zijn overeengekomen.
- 17 Er is een configuratiedossier opgesteld waarin minimaal het volgende is vastgelegd:
  - De verkeersstromen die over netwerkkoppelingen lopen met de daarbij behorende IP protocol, bron- en doel IP adressen, poorten en applicaties;
  - Verantwoordelijkheden, taken en bevoegdheden en contactpersonen van beide partijen;
  - Bij hybride omgevingen, waarbij zowel de leverancier als de ICT-organisatie van Rijkswaterstaat beheerverantwoordelijkheid dragen, is op componentniveau (CI-niveau) vastgelegd hoe de verantwoordelijkheid is verdeeld.
- 18 De applicatie-eigenaar dient conform haar eigen beveiligingsbeleid de authenticiteit van de datastromen en gebruikers vast te stellen.
- 19 De Derde Partij is verplicht registraties bij te houden m.b.t het gebruik van de koppeling en IT-middelen zodat het gebruik is terug te herleiden naar een unieke gebruiker. De Derde Partij moet, indien Rijkswaterstaat aangeeft dat vanaf een bepaald IP-adres op een bepaalde datum en tijd en/of gebruik makende van een bepaald user account, oneigenlijke handelingen verricht zijn op het Rijkswaterstaat netwerk, op verzoek van Rijkswaterstaat per ommegaande de bij deze gegevens behorende gebruikersgegevens terugmelden alsmede maatregelen nemen die noodzakelijkerwijze nodig zijn om misbruik te voorkomen dan wel te beëindigen.

- 20 Informatie uitwisseling rondom beveiligingsincidenten vindt plaats tussen de beveiligingscontactpersonen van beide partijen.
- 21 Beide partijen zullen naar hun beste vermogen samenwerken om operationele problemen die zich voordoen met de end-to-end communicatie op te lossen. Hierbij houdt Rijkswaterstaat zich het recht voor om, indien aangetoond wordt dat het probleem niet aan de zijde van Rijkswaterstaat ligt, vooraf een nader overeen te komen vergoeding voor verdere inzet van haar medewerkers te vragen.
- 22 Wijzigingen worden pas doorgevoerd nadat zij schriftelijk zijn overeengekomen.
- 23 Beide partijen zorgen ervoor dat de verbindingen met publieke netwerken adequaat beveiligd zijn teneinde ongeautoriseerde toegang tot hun en elkaars netwerken te voorkomen.
- 24 De derde partij dient te voorkomen dat andere gekoppelde systemen via hun infrastructuur toegang kunnen verkrijgen tot systemen of de infrastructuur van RWS.
- 25 Beide partijen zullen geen gebruik maken van andere gemeenschappelijke koppelingen dan die zij onderling zijn overeengekomen.
- 26 Indien er gebruik gemaakt wordt van een Ontwikkel-, Test- of Acceptatieomgeving, dient er een strikte scheiding te zijn met de Productie omgeving.
- 27 Beheerverkeer dient gescheiden te zijn van Productie verkeerstromen.
- 28 Om de betrouwbaarheid te waarborgen wordt de omgeving van Rijkswaterstaat bewaakt zonder de integriteit en vertrouwelijkheid of exclusiviteit van de informatie op het informatiesysteem aan te tasten.
- 29 Voor Externe koppelingen worden door Rijkswaterstaat aanvullende veiligheidsmaatregelen genomen, waaronder het filteren op protocollen, IP-adressen, poortnummers en netwerkadresvertalingen.
- 30 Externe koppelingen met het Rijkswaterstaatnetwerk vindt plaats via beveiligde koppelpunten waarbij:
  - Alle in gebruik te nemen externe koppelingen een certificatieproces ondergaan, dat betekent een toetsing conform de eisen in voorliggend document;
  - Koppelingen tussen het interne netwerk van Rijkswaterstaat en een extern netwerk (LAN, WAN) slechts zijn toegestaan indien de beveiliging van dat externe netwerk het beveiligingsniveau van het Rijkswaterstaatnetwerk niet negatief beïnvloedt, dit ter beoordeling van Rijkswaterstaat;
  - Wederzijdse authenticatie en autorisatie is vereist.
- 31 Indien aan een informatiesysteem van de Derde Partij door de Derde partij ook nog zelf een koppeling wordt toegevoegd moet dit worden beschouwd als een



extra risico voor de betrouwbaarheid van het betreffende informatiesysteem en de infrastructuur evenals de informatie die op het informatiesysteem en in de rest van het netwerk verwerkt wordt. Deze risico's dienen door de Derde Partij in kaart gebracht te worden en beoordeeld te worden door Rijkswaterstaat. De Derde Partij neemt alle benodigde additionele maatregelen om deze risico's tot voor Rijkswaterstaat acceptabele niveaus te reduceren. Pas nadat Rijkswaterstaat de Risico's accepteert mogen koppelingen worden toegevoegd.

- 32 Het koppelvlak naar Rijkswaterstaat moet zo ingericht zijn dat de betrouwbaarheid van de informatie en informatievoorziening tijdens transport en verwerking gewaarborgd blijft en dat betrouwbaarheid van andere Rijkswaterstaat informatiesystemen en netwerken gegarandeerd blijven.

### 3 Acceptatie van deze voorwaarden

De ondergetekenden verklaard hierbij dat de in dit document benoemde voorwaarden geaccepteerd worden en gehandhaafd blijven.

Aldus opgemaakt in tweevoud en ondertekend te .....

Datum : .....

Naam en voorletters : .....

Bedrijf : .....

Vestigingsplaats : .....

Emailadres : .....

Telefoon : .....