



RWS INFORMATIE

Software-inkoopvoorwaarden verkeers- en vervoermodellen

WVL VWIV

Datum	27 juni 2025
Versie	1.0
Status	DEFINITIEF

Colofon

Uitgegeven door Rijkswaterstaat
Datum 27 juni 2025
Versie 1.0
Status DEFINITIEF
Rubricering RWS INFORMATIE

Versiebeheer

1.0	DEFINITIEF	27 juni 2025	

Inhoud

Inleiding 4

- 1 Eisen 5**
- 1.1. Werkwijze 5
- 1.2. Standaardisatie 5
- 1.3. Logging 6
- 1.4. Broncode 6
- 1.5. Informatiebeveiliging (BIO) 7
- 1.6. Testen 7
- 1.7. Algemene eisen 8

2 Appendix A: Bronnen 9

Inleiding

Dit document definieert de eisen met betrekking tot softwareontwikkeling voor de modellen rond personen- en goederenvervoer en de gerelateerde applicaties. Het doel is een toepasbaar en onderhoudbaar applicatieportfolio waarbinnen door verschillende (markt)partijen op een uniforme wijze wordt (samen)gewerkt. De inhoud van dit document bevat algemene, niet-functionele voorwaarden en zijn dus niet gericht op een specifiek model of applicatie. Enkele voorwaarden gelden niet voor prototype-ontwikkeling. Als dit het geval is, staat dit vermeld.

In het geval dat eisen uit dit document in tegenspraak zijn met de Algemene Rijksinkoopvoorwaarden voor diensten (ARVODI) of Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT) prevaleert de eerder ARVODI/ARBIT¹ boven de eisen in dit document.

¹ In de uitvraag is aangegeven welk type algemene Rijksinkoopvoorwaarden van toepassing is.

1 Eisen

1.1. Werkwijze

Er zijn verschillende manieren waarop software ontwikkeld kan worden. Ten behoeve van herbruikbaarheid, overdraagbaarheid en onderhoudbaarheid, streven we naar een uniforme werkwijze.

Ww1

Ten behoeve van het issuemanagement, versiebeheer, bouwen, testen, en releasen van software wordt door de Opdrachtnemer een (versie)beheeromgeving (verder te noemen GitLab) gebruikt die door Opdrachtgever ter beschikking wordt gesteld.

Ww2

De Opdrachtnemer gebruikt de in GitLab gedocumenteerde Werkwijzer² als uitgangspunt voor het technisch opzetten en onderhouden van projecten. Daarnaast draagt de Opdrachtnemer actief bij aan deze werkwijzer met voorstellen tot aanpassing. De toegang tot de werkwijzer kan worden aangevraagd via de inhoudelijk projectleider van de Opdrachtgever.

Ww3

Release artifacts worden opgeleverd in de GitLab Registry.

Ww4

Een GitLab pipeline bevat een overzicht met uitgevoerde testen, het resultaat en logging.

Ww5

In de wiki houdt de Opdrachtnemer de projecthistorie bij (per opdracht). Per opdracht wordt het resultaat vastgelegd en de daarbij horende opgepakte GitLab issues.

Ww6

Aanpassingen worden onderworpen aan 4-ogen controle(review). Er wordt dan zowel functioneel/inhoudelijk als technisch naar de aanpassingen (waaronder code en documentatie) gekeken.

Ww7

Functionele en/of technische documentatie en handleidingen worden door Opdrachtnemer bijgewerkt en opgeleverd als er sprake is van nieuwe of gewijzigde functionaliteit. In overleg met de Opdrachtgever kan hiervan worden afgeweken als dat voor de opdracht nodig wordt geacht.

1.2. Standaardisatie

S1

De Opdrachtnemer gebruikt in principe open, gratis en publiek beschikbare standaarden en tools voor ontwikkeling, toepassing (executie), configuratie, interactie (in- en uitvoerbestanden), analyse en documentatie. In overleg met de Opdrachtgever kan hiervan worden afgeweken als dat voor de opdracht nodig wordt geacht.

² <https://gitlab.vv-modellen.nl/documentatie/werkwijzer/>

S2

Voor applicatieconfiguratie wordt bij voorkeur gebruik gemaakt van YAML of JSON. In overleg met de Opdrachtgever kan hiervan worden afgeweken als dat voor de opdracht nodig wordt geacht.

S3

Voor data-uitwisseling wordt gebruik gemaakt van open en actuele formaten. Mogelijkheden zijn bijvoorbeeld GeoPackage en OMX(HDF5). In overleg met de Opdrachtgever worden specifieke keuzes gemaakt.

1.3. Logging**Log1**

Opgeleverde software gebruikt een standaard logging framework met instelbaar loggedrag op basis van configuratie. De output van de logging geeft inzicht in het gedrag van de applicatie.

Log2

Applicatielogging mag niet worden gebruikt als gegevensuitwisselformaat en de logs worden alleen gebruikt voor monitoring, debugging of audits.

1.4. Broncode

De Opdrachtgever stelt als eigenaar van de software eisen met betrekking tot de broncode. Het doel is hier een uniform, veilig, overdraagbaar, herbruikbaar en onderhoudbaar portfolio. In het algemeen wordt voorkeur gegeven aan open source en vrij beschikbare programmeertalen, ontwikkelomgevingen, overige benodigde hulpmiddelen en gestandaardiseerde oplossingen zoals softwarebibliotheken en dataopslag-technologie.

BC1

De Opdrachtnemer betreft de Opdrachtgever bij het maken van keuzes met betrekking tot programmeertalen. Hierbij is het beleid zoals gedefinieerd in de GitLab werkwijzer het uitgangspunt.

BC2

De Opdrachtnemer betreft de Opdrachtgever bij keuzes en mogelijke of nodige verbeteringen met betrekking tot het gebruik van (externe) software bibliotheken, ontwikkelhulpmiddelen, bestandsformaten voor in- en uitvoer of configuratie, en code-standaarden op het gebied van bijvoorbeeld stijl en kwaliteit.

BC3

De Opdrachtnemer gaat bewust om met het gebruik van software (en libraries) van derde partijen en betreft de Opdrachtgever als toepassing gevolgen heeft bijvoorbeeld met betrekking tot licenties, of andere rechten of plichten.

BC4

Door de Opdrachtnemer gewijzigde of toegevoegde broncode wordt opgesteld volgens binnen het project bestaande style en/of layout afspraken. Voor zover mogelijk wordt geautomatiseerd statische code analyse toegepast.

BC5

De broncode wordt automatisch vanuit de GitLab pipeline verstuurd naar Sigrid ter analyse³. Nieuwe projecten hebben kwaliteitsscores van minimaal 3,5 uit 5 op het gebied van onderhoudbaarheid, architectuur, open source health, veiligheid en betrouwbaarheid. In bestaande projecten met een score lager dan 4 uit 5 mogen kwaliteitsscores niet verslechteren. Deze eis is niet van toepassing voor ontwikkeling van prototypes.

³ <https://sigrid-says.com/rijkswaterstaat/>

1.5. Informatiebeveiliging (BIO)

IB1

De Opdrachtnemer is bekend met de [BIO] (Zie Appendix A) en de daarin gedefinieerde basisbeveiligingsniveaus. Tenzij anders overeengekomen, is in de opdracht BBN1 van toepassing.

IB2

De verantwoordelijkheid voor de naleving van de [BIO] ligt bij de Opdrachtgever. De Opdrachtnemer zal de Opdrachtgever informeren als er naar diens oordeel niet wordt voldaan aan het beoogde beveiligingsniveau.

IB3

De Opdrachtnemer past de volgende overheidsmaatregelen uit de [BIO] toe. Dit is een selectie van de maatregelen waarvan de implementatie uitgevoerd wordt door de Opdrachtnemer.

1. Maatregelen m.b.t. logging van online services.
 - a. 12.4.1.1
Een logregel bevat minimaal:
 - (a) de gebeurtenis;
 - (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
 - (c) het gebruikte apparaat;
 - (d) het resultaat van de handeling;
 - (e) een datum en tijdstip van de gebeurtenis.
 - b. 12.4.1.2
Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
 - c. 12.4.2.1
Er is een overzicht van logbestanden die worden gegenereerd.
 - d. 12.4.2.2
Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
2. Security
 - a. 14.2.1.1
De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.
Dit leggen we zodanig uit dat security meegenomen moet worden vanaf de start van het project en niet pas aan het einde.
 - b. 14.2.6.1
Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.

IB4

Credentials zoals gebruikersnamen en wachtwoorden worden opgeslagen middels daartoe bestemde opslagmechanismes. Indien deze nodig zijn, wordt in overleg met de Opdrachtgever een passende oplossing worden gekozen.

1.6. Testen

Test1

Broncode van het project wordt voor zover redelijkerwijs mogelijk via de pipeline getest met behulp van unittesten. De testcoverage van *gewijzigde* code is minimaal

75 procent. Deze eis is niet van toepassing voor ontwikkeling van prototypes en user interfaces.

Test2

Met behulp van integratietesten wordt geverifieerd dat alle componenten of modules samenwerken zoals verwacht. Bij integratietesten ligt de focus op functionele compleetheid. Code coverage is hierbij geen doel, maar kan gebruikt worden om vast te stellen dat de functionaliteit daadwerkelijk gebruikt wordt, of dat er integratietesten ontbreken. Deze eis is niet van toepassing voor ontwikkeling van prototypes en user interfaces.

Test3

Automatische testen maken gebruik van kleine en eventueel synthetische invoerbestanden die bij voorkeur automatisch zijn gegenereerd. De daarvoor benodigde data, code, scripts en bijbehorende documentatie staan in GitLab zodat het mogelijk is later opnieuw testdata te genereren. Deze eis is niet van toepassing voor ontwikkeling van prototypes en user interfaces.

1.7. Algemene eisen

Alg1

De Opdrachtnemer overlegt met de Opdrachtgever indien in het licht van de opdracht en of gestelde eisen in dit document keuzes of beslissingen nodig worden geacht.

Alg2

De Opdrachtnemer adviseert Opdrachtgever gedurende de looptijd van de opdracht vrijblijvend over mogelijkheden tot verbetering van deze voorwaarden of (werk)inhoudelijke processen indien daar aanleiding voor is.

2 Appendix A: Bronnen

Kenmerk	Bron	Beschikbaarheid
[BIO]	Baseline Informatiebeveiliging Overheid versie 1.04zv	Openbaar