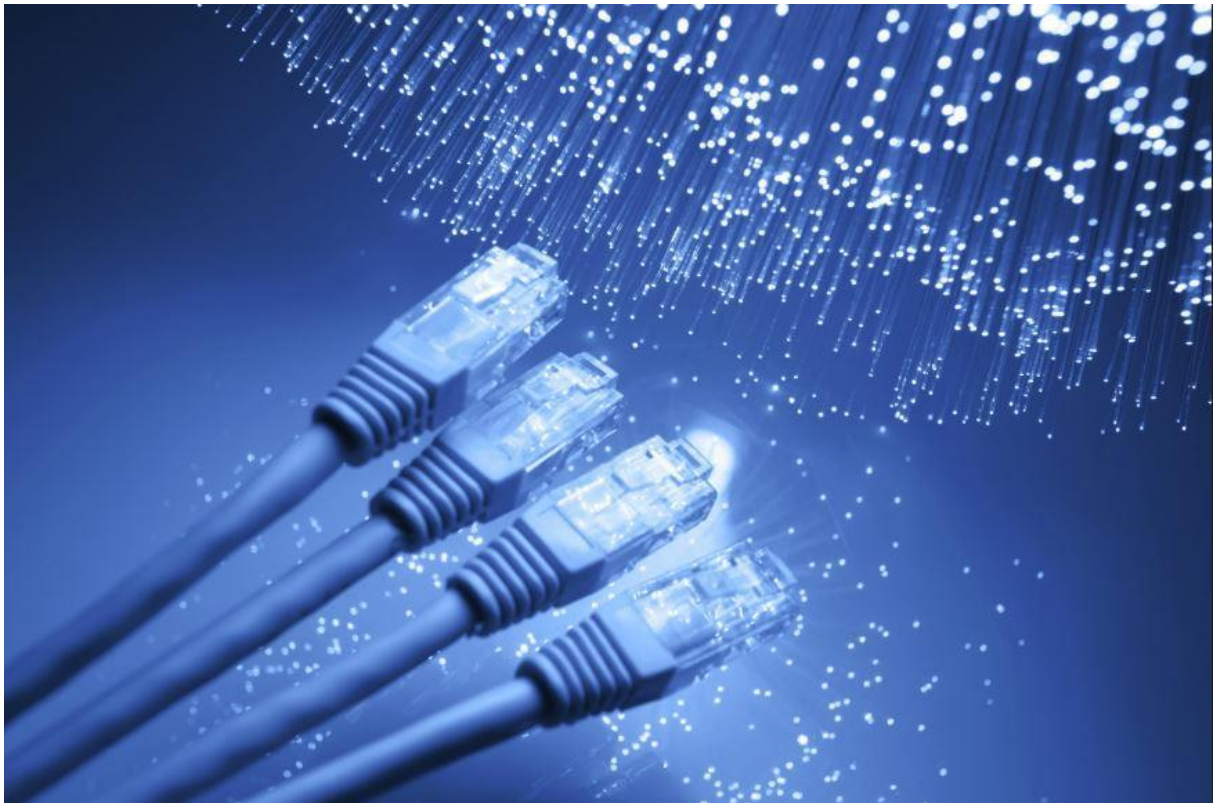




ICT Vereisten Waterschap Rijn en IJssel

HARD- EN SOFTWARE, SECURITY EN PRIVACY

W. Oonk | versie 1.8 | 23-04-2026

Algemeen

Voor het in gebruik nemen van nieuwe of vervangende software op servers en werkstations bij waterschap Rijn en IJssel (WRIJ), heeft de unit ICT de volgende eisen opgesteld. Software welke niet voldoet aan de in dit document minimaal gestelde eisen zal niet worden geïmplementeerd. Het waterschap volgt de BIO normering en de Wettelijk verplichte (open) standaarden van de Digitale overheid.

Inhoud

Algemeen.....	2
Hard- en Software vereisten waterschap Rijn en IJssel	3
Server	3
Applicatie / Database Server	3
WebServer	3
Server Based Computing	4
Werkstation en applicaties.....	4
Netwerk.....	4
SaaS	5
Aanvullende technische eisen en randvoorwaarden.....	6
Beveiliging	8
Persoonsgegevens.....	8

Hard- en Software vereisten waterschap Rijn en IJssel

Server

Standaard wordt gebruik gemaakt van virtuele servers tenzij essentiële functionaliteit in de applicatie verloren gaat.

Operating system:	Windows Server 2025 of hoger Linux Ubuntu 24.04 LTS
Virtualisatie:	VMWare ESX 9.0 of hoger
Informatieveiligheid	Hardening volgens Microsoft principes (security baseline) worden op windows servers toegepast.

Applicatie / Database Server

De applicatie die wordt geselecteerd moet kunnen werken met de volgende applicatie-/databaseserver hard- en software:

Operating system:	Windows Server 2025 of hoger Linux Ubuntu 24.04 LTS
Database:	Microsoft SQL Server 2025 of hoger, PostgreSQL 18.3 of hoger, Oracle 19c of hoger (wordt uitgefaseerd),
Virtualisatie:	VMWare ESX 9.0 of hoger
Service accounts	Via gMSA (Group Managed Service Account)
Certificaten	SSL Certificaat worden geautomatiseerd vervangen. Bv. ACME DNS-01 challenge, API, script, ect.
Informatieveiligheid	Microsoft Security Baseline en ASR Rules moeten worden toegepast. Hardening volgens Microsoft principes (security baseline) worden op windows servers toegepast.

WebServer

De applicatie die wordt geselecteerd moet kunnen werken met de volgende webserver hard- en software:

Operating system:	Windows Server 2025 of hoger Linux Ubuntu 24.04 LTS
Applicaties:	Microsoft IIS
Virtualisatie:	VMWare ESX 9.0 of hoger
Informatieveiligheid	Hardening volgens Microsoft principes (security baseline) worden op windows servers toegepast.

Server Based Computing

Applicaties bedoelt voor thuiswerken of decentrale locaties zijn door de leverancier gecertificeerd en ondersteund voor:

Citrix Virtual Apps and Desktops:	versie 2507 LTSR
-----------------------------------	------------------

Werkstation en applicaties

De applicatie die wordt geselecteerd moet kunnen (samen)werken met de volgende werkstation hard- en software:

Hardware client:	Intel Pentium i5 Gen 7, 16 GB intern geheugen, 260 GB HD, beeldscherm 1920 x 1080 of beter
Operating system:	Windows 11 (64-bit)
Applicaties:	zijn programmeer-technisch opgezet volgens de methodiek van Microsoft, distributie naar werkstations geschied via SCCM en/of Microsoft Intune
Browser:	MS Edge of Chrome. De laatste versie
Werkstations specs VDI omgeving	Stateless nu: 4 vCPU 12GB geheugen 1GB video 120GB disk Stateless in 2027: 6 vCPU 16GB geheugen 2GB video 120GB disk
informatieveiligheid	Microsoft Security Baseline en ASR Rules moeten worden toegepast. Microsoft Defender for Endpoint wordt toegepast

Netwerk

Netwerkprotocol:	TCP/IP
Domein:	Microsoft Windows 2022
Authenticatie:	Via AD of EntraID, SSON (buiten netwerk WRIJ)
Wachtwoorden:	Default wachtwoorden dienen te worden gewijzigd en opgeslagen in de kluis bij systeembeheer. Wachtwoorden bestaan uit minimaal 12 karakters en bestaan uit hoofd- en kleine letters, cijfers en vreemde tekens (conform BIO-norm).

Routing	Vindt altijd plaats via centrale omgeving WRIJ.
---------	---

SaaS

Zie hiervoor het document “Vereisten cloud dienst Waterschap Rijn en IJssel”.

Aanvullende technische eisen en randvoorwaarden

1. De software moet tenminste de komende (5) jaar door de leverancier ondersteund worden.
2. De server-software dient het gelijktijdig gebruik vanaf meerdere werkstations te ondersteunen (multi-user).
3. De software dient bij voorkeur web based en anders volledig client-server (multi-tier) te zijn.
4. De software moet via Microsoft Windows Installer (MSI)/SCCM te installeren zijn.
5. De software behoeft geen local admin rechten voor werking.
6. Default accounts moeten worden aangepast. No-named user accounts zijn niet toegestaan.
7. Default wachtwoorden worden aangepast en bestaan dan uit minimaal 12 karakters, hoofd- en kleine letters, cijfers en vreemde tekens (conform BIO=norm).
8. De software dient te beschikken over zo breed mogelijke faciliteiten voor data-uitwisseling met andere software. D.m.v. open standaarden (zoals SOAP, UDDI, WSDL, XML, OLE/COM, ODBC, DDE) moeten gegevens met andere systemen uitgewisseld kunnen worden (zowel import als export) en/of koppelingen met andere informatiesystemen en databases gerealiseerd kunnen worden.
9. Het gebruik van de software en database op de server(s) op het hoofdkantoor, moet mogelijk zijn vanuit de werkplekken op het hoofdkantoor en vanuit elke willekeurige locatie buiten het hoofdkantoor via Citrix Virtual Apps and Desktops.
10. Nieuwe versies van de programmatuur moeten tijdig door de leverancier aangekondigd worden. Daarbij moeten eventuele consequenties voor (de capaciteit van) de technische infrastructuur, voor de door de leverancier geleverde maatwerkprogrammatuur en voor de door de leverancier geleverde koppelingen met andere systemen (van derden) vermeld worden.
11. De leverancier moet op verzoek van Waterschap Rijn en IJssel tijdig nieuwe versies van geleverd maatwerk en van geleverde koppelingen met andere systemen opleveren. Zowel gewijzigde software van de leverancier als gewijzigde software van derden kunnen dit noodzakelijk maken. Als Waterschap Rijn en IJssel echter nog geen behoefte heeft aan nieuwe versies van andere systemen (van derden), dient het geleverd maatwerk en dienen de geleverde koppelingen te blijven functioneren en daartoe eventueel aangepast te worden. Als voorbeeld kunnen koppelingen met het centraal gegevensverwerkend systeem, met het onderhoudsbeheersysteem en met MS Office genoemd worden.
12. De software moet indien nodig ge(her)installeert kunnen worden door systeembeheerders van Waterschap Rijn en IJssel en de te leveren installatiehandleiding. Een training-on-the-job moet daarvoor voldoende informatie geven.
13. Voor zover applicatie- en systeembeheerders van Waterschap Rijn en IJssel betrokken moeten zijn bij het technisch beheer van de te leveren software en/of databases, moeten daarvoor beheerdershandleidingen geleverd worden.
14. Bij de leverancier dient een helpdesk of aanspreekpunt voor de applicatie- en systeembeheerders van Waterschap Rijn en IJssel bereikbaar te zijn, die tijdens kantooruren binnen 1 werkdag antwoord kan geven op technische vragen. Benodigde SLA geschied in overleg.
15. Voor het gebruik van de software moet voor eindgebruikers een deugdelijke gebruikershandleiding geleverd worden.
16. Als bijlage bij offertes moet een gedetailleerd overzicht van de capaciteit van de benodigde hardware en communicatievoorzieningen geleverd worden. Waterschap Rijn en IJssel behoudt zich het recht voor om deze hardware en/of communicatievoorzieningen in eigen beheer te realiseren en te beheren.

17. Als bijlage bij offertes moet een gedetailleerd overzicht van de kenmerken en de capaciteit van alle geoffreerde onderdelen geleverd worden.
18. Tooling benodigd voor implementatie kan tijdens de test periode worden geïnstalleerd indien deze tooling actueel is en wordt gepatcht. Na de test periode wordt de tooling verwijderd door de engineer die de software heeft geïnstalleerd.
19. Alle systemen vallen onder het standaard domein van WRIJ. Uitzondering hierop vormt de Procesautomatisering.
20. Voor beheer of toegang op afstand tot systemen van het waterschap wordt alleen gebruik gemaakt van Privileged Remote Access (PRA – Beyond Trust).
21. Nieuwe benodigde hardware en/of software wordt aangevraagd via de Topdesk omgeving van het waterschap.
22. Elke applicatie heeft 2 applicatie/functioneel beheerders en een eigenaar (van het waterschap) voordat deze in beheer door het waterschap kan worden genomen. Er vindt altijd overdracht naar de beheerorganisatie plaats.
23. Daar waar generative AI (agents en/of model) voor software wordt toegepast wordt deze vooraf en in duidelijke taal aan het waterschap kenbaar gemaakt. Het moet duidelijk worden in welk proces wordt ingehaakt, welke data wordt geraadpleegd en hoe data wordt getransporteerd en waarnaartoe.
24. Kwetsbaarheden in software worden gemeld bij de Servicedesk ICT (Security@wrij.nl). De leverancier is hiervoor verantwoordelijk en zorgt ervoor dat bij hoge of kritieke CVSS scores (zie [NCSC NL | Security Advisories](#)) binnen 10 werkdagen een passende patch wordt geïnstalleerd.

Beveiliging

Het waterschap hanteert de BIO als Normenkader. Keywords zijn hierin 'Security by Design' en 'Defense indept'. Dat betekent onder andere dat systemen hardened worden uitgevoerd volgens de standaard van Microsoft en worden gedocumenteerd voordat overdracht naar de beheer organisatie (systeembeheer ICT-WRIJ) kan plaatsvinden. Hierdoor dient vooraf alle benodigde (systeem-)software en instellingen bij de beheer organisatie bekend te zijn.

Certificaten, Audit verslagen en/of PEN-test rapporten moeten indien van toepassing ook daadwerkelijk vooraf worden getoond of kopieën overhandigd. Voor implementatie wordt duidelijk gemaakt welke certificaten benodigd zijn en van welk type.

Koppelingen met andere systemen of internet/cloud worden vooraf door de leverancier kenbaar gemaakt. Daar waar encryptie van belang is wordt deze toegepast en vooraf besproken en beschreven door de leverancier.

De leverancier overhandigd na oplevering een configuratiedocument op. Daarin zit minimaal:

1. architectuur plaat (systeemniveau);
2. namen van systemen;
3. software versies;
4. controle uitgevoerde hardening
5. certificaten;
6. namen van (service-) accounts;
7. definieerbare rollen
8. koppelingen
9. firewall wijzigingen;
10. DNS aanpassingen;
11. Uit te voeren scripting;
12. folder structuur en systeemtaken.

Persoonsgegevens

Indien persoonsgegevens in het systeem voorkomen, dienen de volgend vragen te worden beantwoord:

1. Voor welk doel worden persoonsgegevens gevraagd:
2. Welke type persoonsgegevens worden gevraagd:
3. Worden niet meer dan nodig persoonsgegevens verzameld?
4. Worden persoonsgegevens verstrekt aan derden?
5. Hoe lang worden persoonsgegevens bewaard?
6. Welke maatregelen zijn getroffen voor het voorkomen van verlies, verminking of ongeoorloofde inzage van persoonsgegevens?

In geval van verwerking van persoonsgegevens volgt een PIA (Privacy Impact Analyse) en zal een Verwerkersovereenkomst worden opgesteld.

De data of andere informatie van het waterschap staat indien van toepassing op servers in de EU.