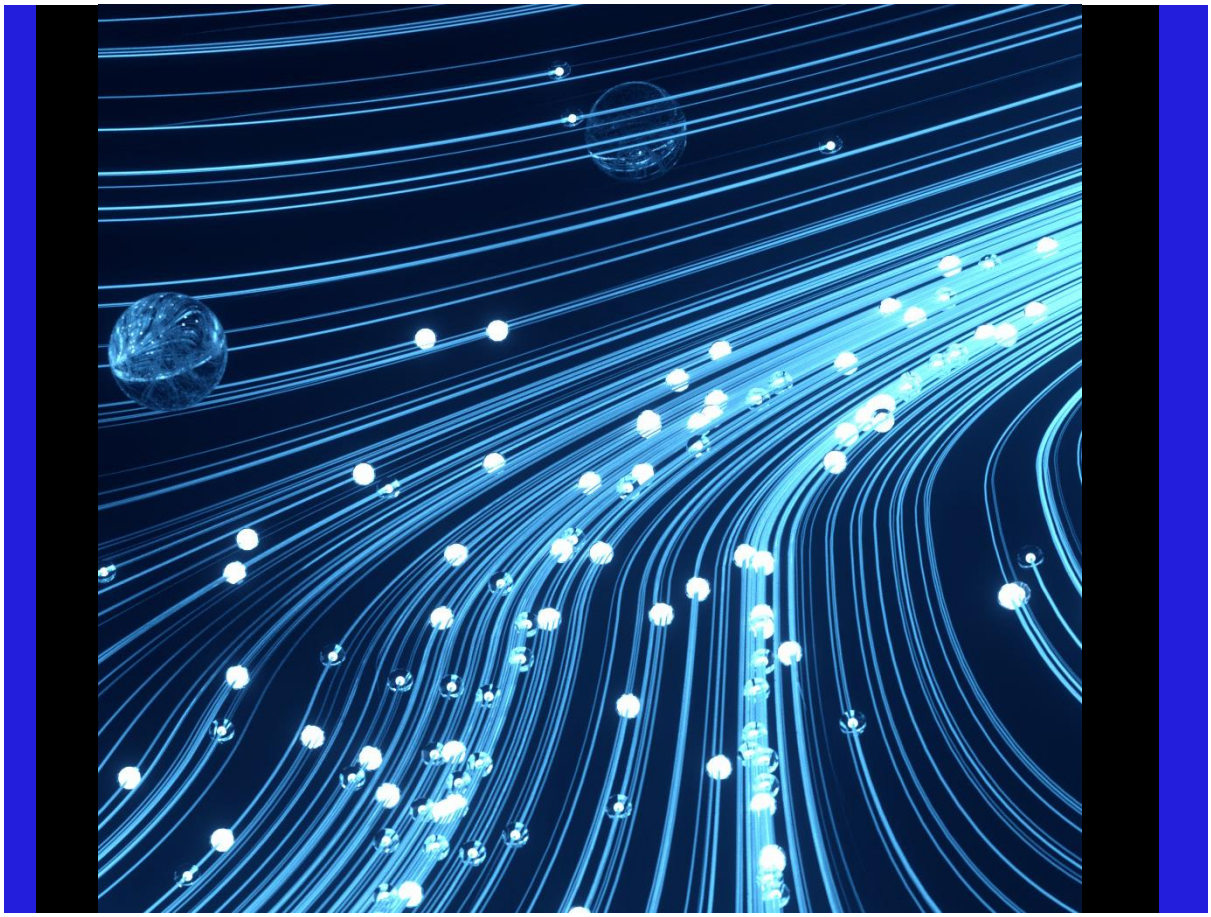
Service Definition Document – Water Works

Document no: 001
Revision: v1.0

CCS - G-Cloud 15
21 January 2026



Service Definition Document – Water Works

Client name:	n/a		
Project name:	CCS - G-Cloud 15		
Client reference:	n/a	**Project no:**	n/a
Document no:	001	**Project manager:**	Hugh McMichael
Revision:	v1.0	**Prepared by:**	n/a
Date:	21 January 2026	**File name:**	GCloud15_ServiceDef_WaterWorks

Document history and status

Revision	Date	Description	Author	Checked	Reviewed	Approved

Distribution of copies

Version	Issue approved	Date issued	Issued to	Comments

Jacobs U.K. Limited

Cottons Centre
Cottons Lane
London SE1 2QG
United Kingdom

T +44 (0)203 980 2000
www.jacobs.com

© Copyright 2026 Jacobs U.K. Limited. All rights reserved. The content and information contained in this document are the property of the Jacobs group of companies ("Jacobs Group"). Publication, distribution, or reproduction of this document in whole or in part without the written permission of Jacobs Group constitutes an infringement of copyright. Jacobs, the Jacobs logo, and all other Jacobs Group trademarks are the property of Jacobs Group.

NOTICE: This document has been prepared exclusively for the use and benefit of Jacobs Group client. Jacobs Group accepts no liability or responsibility for any use or reliance upon this document by any third party.

Contents

Service attributes

Service type

Lot 2b: Software as a Service (SaaS)

Service name

Service name

Water Works

About your service

Service description

Easy-to-use and flexible User Interface to leverage the power of Pywr water resources modelling software and cloud-based computing. Helps create, review and edit scenario data, initiate four different types of model runs and review results of scenarios modelled with Pywr.

Service categories

- Applications
  - Production and operations
    - Service industry and public sector operations
      - Defense
      - Other
    - Other operations
      - Other operations

Multi cloud support

Yes

Service features and benefits

Service features and benefits

Service features

- Easy-to-use User Interface plugged to client Pywr model
- Create, edit and model multiple Water Resources scenarios

- Efficient scenario cloning and customisation
- Display daily time series results for 100+ years of simulation
- Display yearly heatmap failure for 19,200 years of stochastic modelling
- Modifications to data are flagged in a scenario
- Input data can be traced to source
- Fully hosted web service utilising a robust cloud platform
- Configurable to add on custom dashboards
- Extendable to include multi-objective optimisation

Service benefits

- Removes reliance on external consultants
- Removes reliance on developers to run Pywr models
- Configurable, adaptable and scalable database
- Easy review and comparison of scenario results
- Assess and compare future water resources solutions
- Efficient and proactive production planning decisions
- Analytics to manage through drought situations

Service scope

Add-ons and extensions

Software add-on or extension

No

Cloud deployment model

Public cloud

Service constraints

Works with a Pywr model only

System requirements

Access to supported web browser

Reselling

Supplier type

Supplier type

I'm not a reseller

User support

Email or ticketing support

Email or online ticketing support

Yes

Support response times

SLA's to be agreed with client

User can manage status and priority of support tickets

No

Phone support

Phone support

Yes

Phone support availability

9 to 5 (UK time), Monday to Friday

Web chat support

Web chat support

No

Onsite support

Yes, at extra cost

Support levels

SLA's to be agreed with clients

Support available to third parties

Yes

How users work with your service

Browsers

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Chrome
- Safari

Installation

Application to install

No

Mobile

Designed for use on mobile devices

No

Differences between the mobile and desktop service

Track Record is built as a responsive web application and will dynamically reposition the UI to suit desktop, tablet and phone resolutions.

Service interface

Service interface

Yes

Description of service interface

The user interface is accessible through a supported browser.

Accessibility standards

EN 301 549

Accessibility testing

No testing undertaken yet

User support

User support accessibility

None or don't know

API

API

No

Customisation

Customisation available

Yes

Description of customisation

Clients can customise their terminology and select specific modules These would be made on client's behalf by Jacobs

Onboarding and offboarding

Getting started

During the mobilisation phase we tailor and configure WaterWorks to client requirements. This includes providing technical support to connect the user interface to the client's Pywr model. User training can be delivered onsite, online or a combination of both. The interface has User Guide that details the functionality. We also provide guidance during start up on the best technical approach to achieve the water resources modelling goal.

Documentation

Service documentation

Yes

Documentation formats

PDF

Documentation accessibility standard

None or don't know

How the documentation is accessible

Accessibility needs can be reviewed and adjustments made as required.

End-of-contract data extraction

Data can be downloaded at the end of a contract and the format and method can be agreed with the client during off-boarding.

End-of-contract process

The demobilisation of Water Works consists of a download and export of data held, in an agreed format. These costs are not included in the price range quoted in the pricing document, but can be agreed at extra cost.

Data importing and exporting

Data export approach

Technical support is available should a mass download of data be required in a particular format.

Data export formats

Data export formats

- CSV
- Other

Other data export formats

- JSON
- XLSX
- PNG

Data import formats

Data import formats

- CSV
- Other

Other data import formats

XLSX

Analytics

Metrics

Service usage metrics

Yes

Metrics types

Modules within the tool to show user activity, e.g. logins, recent activity, etc.

Reporting types

Reports on request

Resource tagging

No

FOCUS resource tagging

No

Scaling

Independence of resources

All clients data is separated by database row level security. Separate databases can be implemented for separate clients on request.

Public sector networks

Public sector networks

Connection to public sector networks

No

Data-in-transit protection

Protection between networks

Data protection between buyer and supplier networks

TLS (Version 1.2 or above)

Protection within your network

Data protection within supplier network

TLS (Version 1.2 or above)

Asset protection

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

United Kingdom

User control over data storage and processing locations

Yes

Datacentre security standards

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Penetration testing

Penetration testing frequency

At least once a year

Penetration testing approach

Another external penetration testing organisation

Protection of data at rest

Protecting data at rest

- Physical access control, complying with SSAE-18 / ISAE 3402
- Encryption of all physical media

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

Deleted data can't be directly accessed / Cryptographic Erasure

Equipment disposal approach

A third-party destruction service

Availability and resilience

Guaranteed availability

SLAs to be agreed with clients.

Approach to resilience

Jacobs Digital has a "Cloud First" policy for all technical solutions we implement. We take a vendor agnostic approach when proposing solutions and will work with whichever provider makes the most sense for our clients. We are currently using MS Azure for hosting. MS Azure and is fully accredited for ISO 9001, 27001 and 20000.

Outage reporting

We use an external automated monitoring service to continually ensure our services are operational. In the event of any downtime or glitch the technical support team are notified by SMS and email.

Governance

Named board-level person responsible for service security

Yes

Security governance

Software Security Code of Practice

Yes

Security governance certified

Yes

Security governance standards

- ISO/IEC 27001
- Other

Other security governance standards

ISO9001, ISO14001, ISO45001 and SSIP LRQA Registration Certificate NIST CSF ISO27001 Cyber Essentials Plus

Information security policies and processes

Information Security Policies & Processes We operate under a Global Security Policy, UK Information Security Policy, and Global Data Protection Policy, all supported by ISO 27001 and Cyber Essentials Plus accreditation. Our Security Operations Centre provides 24/7 monitoring of networks, servers, and endpoints. Access to information is governed by "need-to-know" principles, with controls such as classified document registers, secure transfer protocols, clear-desk policies, and documented backup/recovery procedures. All staff undergo annual security awareness training, sign acceptable-use policies, and complete BPSS vetting with

controlled office access. Reporting Structure Security oversight is led by a Board-level Senior Information Risk Owner (SIRO), supported by a Group Security Controller (GSC) and a Corporate Security Team. The named Security Controller for UK/B&I Europe is Steve Colwill. Ensuring Adherence We ensure compliance through regular risk-register reviews, incident reporting and updates, IT governance and internal audit, and by aligning suppliers with our security procedures. These measures collectively maintain robust information security and policy adherence across the organization.

Operational security

Configuration and change management standard

Supplier-defined controls

Configuration and change management approach

Jacobs employs a robust Configuration and Change Management Standard to ensure consistency, traceability, and control over its projects and systems. This standard is crucial for maintaining the integrity of our operations and delivering high-quality services to our clients. Key aspects of the standard include: Configuration Management, Change Management, Version Control, Documentation, Approval Processes, Risk Assessment, Auditing and Compliance, and Training This standard helps Jacobs maintain consistency across projects, reduce errors, improve efficiency, and ensure that changes are implemented in a controlled and traceable manner, ultimately contributing to the success of our projects and client satisfaction.

Vulnerability management type

Supplier-defined controls

Vulnerability management approach

Jacobs ensures robust security through a multi-layered approach: frequent vulnerability scans (daily for development, weekly for networks, monthly for production, quarterly for infrastructure), comprehensive penetration testing (annual internal, bi-annual external, continuous via bug bounty), and structured patch management (critical within 24 hours, high-risk in 7 days). Third-party software risks are mitigated through inventory control, automated vulnerability monitoring, strict version policies, and vendor communication. Specialized tools like Software Composition Analysis streamline these processes. This proactive strategy enables Jacobs to identify and remediate vulnerabilities quickly, maintain compliance, and minimize risk for both the organization and its clients.

Protective monitoring type

Supplier-defined controls

Protective monitoring approach

Jacobs' protective monitoring processes employ advanced threat detection systems, regular vulnerability scans, and 24/7 SOC monitoring to identify potential compromises. When a threat is detected, we initiate a structured response plan including immediate containment, in-depth investigation, and swift remediation. Our incident response time is prioritized based on severity, with critical incidents addressed within 15-30 minutes. A dedicated team is available round-the-clock for urgent matters, supported by automated systems

for quick isolation of affected areas. Regular drills ensure our team maintains rapid response capabilities, adapting to evolving cybersecurity challenges.

Incident management type

Supplier-defined controls

Post-quantum cryptography secure

No

Incident management approach

Jacobs ensures rapid response and resilience through a structured approach:

- Identification & Response: Automated detection, 24/7 SOC monitoring, tiered escalation, and incident-specific playbooks.
- Communication: Internal and external notifications, regulatory compliance.
- Roles: Incident Response Manager, Technical Lead, Communications Lead, Legal Counsel, Executive Sponsor.
- Timelines: Critical incidents addressed within 15 minutes; others within defined hours.
- Threat Intelligence Sharing: Real-time dashboards, client portals, ISAC participation, collaborative exercises.
- Root Cause Analysis: RCA for High/Critical incidents, remediation plans, continuous improvement reviews.
- Business Continuity: Comprehensive BCP/DR plans, redundant systems, regular testing and audits.

Staff security

Staff security clearance

Staff screening performed which conforms to BS7858:2019

Government security clearance

Up to Baseline Personnel Security Standard (BPSS)

Secure development

Approach to secure software development best practice

Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v4.0)

Identity and authentication

User authentication

User authentication needed

Yes

User authentication

- Multi-Factor Authentication (MFA)
- Identity federation with existing provider (for example Google apps)
- Username or password

Access restrictions in management interfaces and support channels

Water Works has an admin interface accessed by the Jacobs support team that enables full control of user and user team access to modules and user rights (e.g. ability to edit or delete). User access can be locked upon request by the client or if there is no user activity for a specified period of time (6 months) then the user account is automatically locked.

Access restriction testing frequency

At least every 6 months

Management access

Management access authentication

- Multi-Factor Authentication (MFA)
- Identity federation with existing provider (for example Google apps)
- Username or password

Audit information for users

Audit for buyers' users' actions

Access to user activity audit information

Users contact the support team to get audit information

How long user audit data is stored for

At least 12 months

Audit for suppliers' users' actions

Access to supplier activity audit information

Users contact the support team to get audit information

How long supplier audit data is stored for

At least 12 months

How long system logs are stored for

At least 12 months

Pricing

Discount for educational organisations

No

Free or trial versions

Free trial available

No