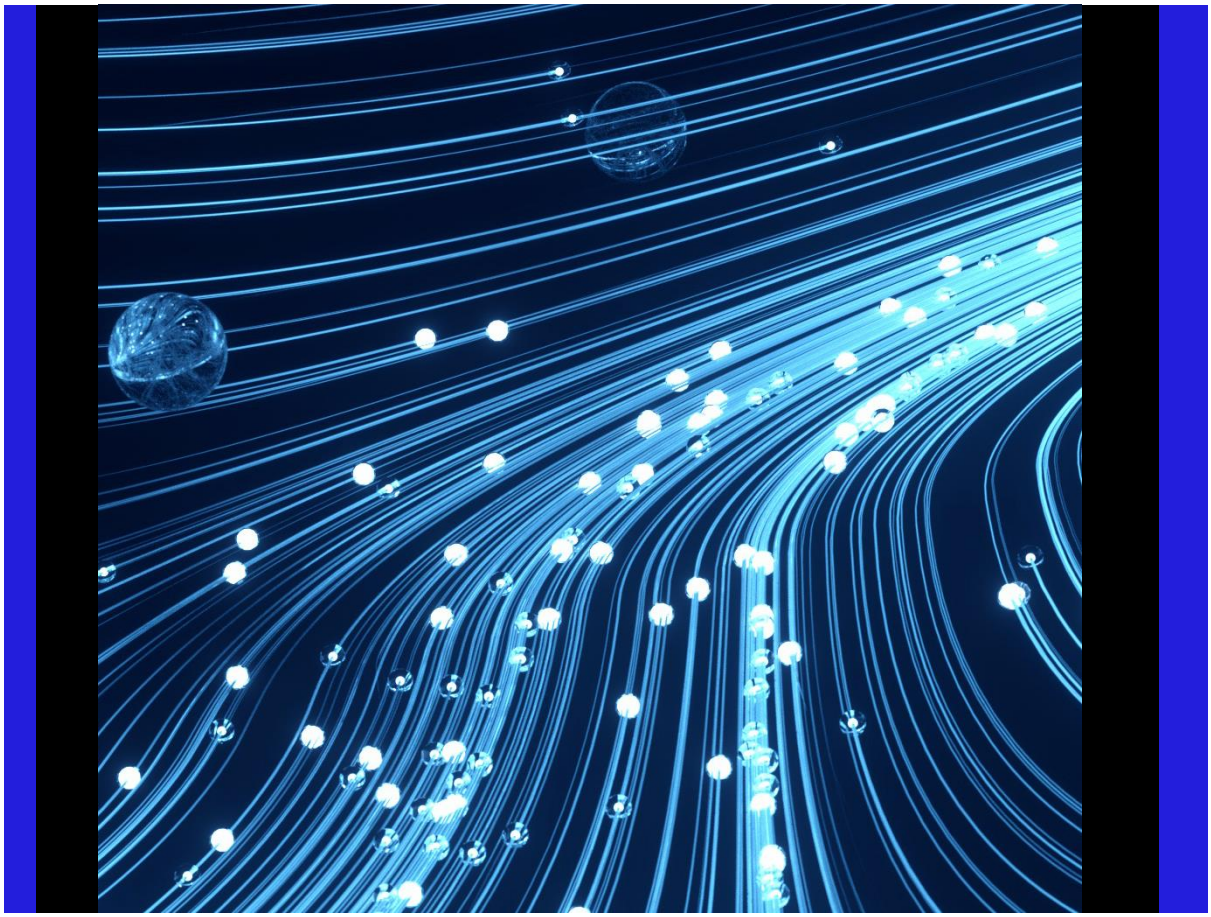
Jacobs

Service Definition Document – Aqua DNA

Document no: 001
Revision: v1.0

CCS - G-Cloud 15
19 January 2026



Service Definition Document – Aqua DNA

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:	19 January 2026	**File name:**	GCloud15_ServiceDef_AquaDNA

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

Contents

Service attributes **6**
Service type 6
Service name **6**
Service name 6
About your service **6**
Service description 6
Service categories 6
Multi cloud support 6
Service features and benefits **7**
Service features and benefits 7
Service scope **7**
Add-ons and extensions 7
Cloud deployment model 7
Service constraints 8
System requirements 8
Reselling **8**
Supplier type 8
User support **8**
Email or ticketing support 8
Phone support 8
Web chat support 9
Onsite support 9
Support levels 9
Support available to third parties 9
How users work with your service **9**
Browsers 9
Installation 9
Mobile 9
Service interface 10
User support 10
API 10
Customisation 11
Onboarding and offboarding **11**
Getting started 11
Documentation 11
End-of-contract data extraction 11
End-of-contract process 11

Data importing and exporting **12**
Data export approach 12
Data export formats 12
Data import formats 12
Analytics **12**
Metrics 12
Scaling **13**
Independence of resources 13
Public sector networks **13**
Public sector networks 13
Data-in-transit protection **13**
Protection between networks 13
Protection within your network 13
Asset protection **13**
Data storage and processing locations 13
Datacentre security standards 14
Penetration testing 14
Protection of data at rest 14
Data sanitisation process 14
Equipment disposal approach 14
Availability and resilience **14**
Guaranteed availability 14
Approach to resilience 15
Outage reporting 15
Governance **15**
Named board-level person responsible for service security 15
Security governance 15
Information security policies and processes 15
Operational security **16**
Configuration and change management standard 16
Configuration and change management approach 16
Vulnerability management type 16
Vulnerability management approach 16
Protective monitoring type 16
Protective monitoring approach 16
Incident management type 16
Post-quantum cryptography secure 17
Incident management approach 17

Staff security **17**
Staff security clearance 17
Government security clearance 17
Secure development **17**
Approach to secure software development best practice 17
Identity and authentication **17**
User authentication 17
Access restrictions in management interfaces and support channels 18
Access restriction testing frequency 18
Management access 18
Audit information for users **18**
Audit for buyers' users' actions 18
Audit for suppliers' users' actions 18
How long system logs are stored for 19
Pricing **19**
Discount for educational organisations 19
Free or trial versions 19

Service attributes

Service type

Lot 2b: Software as a Service (SaaS)

Service name

Service name

Aqua DNA

About your service

Service description

Asset performance monitoring platform for pumping station and sewer network management combining cloud analytics platform with IoT sensors. Aqua DNA enables wastewater network operators to access real time and reliable asset performance data and predictive insight, thus optimising asset performance, and allowing efficient and proactive asset management and investment decisions.

Service categories

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

Multi cloud support

Yes

Service features and benefits

Service features and benefits

Service features

- Real time asset performance data collated though IoT every 20'
- Real time asset data displayed in monitoring dashboard
- Predictive analysis of asset future performance using ML
- Display of data for over 30,000 number assets
- Visualisation of sewerage assets through mapping
- Smart maintenance programme
- Fully hosted web service utilising a robust cloud platform
- Configurable workflows with events and alerting

Service benefits

- Significant reduction in maintenance spend
- Collation of reliable asset performance data
- Access to real time asset performance and health assessment
- Insight in future asset performance
- Asset performance optimisation
- Efficient and proactive asset management and investment decisions
- Increase in pump life expectancy
- Reduction in number of pumping station overflows (flooding)
- Energy savings
- Configurable, adaptable and scalable database

Service scope

Add-ons and extensions

Software add-on or extension

No

Cloud deployment model

Public cloud

Service constraints

Platform requires sensors to collect data to feed into platform (Telemetry or IOT sensors)

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 can be agreed with clients

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

None or don't know

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
- Firefox
- Chrome
- Safari
- Opera

Installation

Application to install

No

Mobile

Designed for use on mobile devices

No

Service interface

Service interface

Yes

Description of service interface

The user interface is accessible through a supported browser. + Service Now ticketing system for first line support

Accessibility standards

EN 301 549

Accessibility testing

No testing undertaken yet

User support

User support accessibility

None or don’t know

API

API

Yes

What users can and can't do using the API

Aqua DNA through its user-friendly web-based API. With Aqua DNA, users can perform a wide range of tasks based on their access level, all within an intuitive Web interface. Aqua DNA’s flexible ingest platform allows seamless integration of real-time data from various sources. Whether it’s data posting, periodic retrieval through APIs, or working with intermediary services like FTP, SFTP, or Cloud Storage, Aqua DNA efficiently handles it all. By leveraging existing sensors, SCADA systems, and third-party analytics.

API documentation

Yes

API documentation formats

Open API (also known as Swagger)

API sandbox or test environment

No

Customisation

Customisation available

Yes

Description of customisation

Clients can customise their terminology, integration with existing data sets, 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 Aqua DNA to client requirements. This includes providing technical support to import client data and technical reviews co-ordinated by a dedicated Project Manager for best practice use of the tools. User training can be delivered onsite, online or a combination of both. The tools have online documentation and user help and we also provide user guidance in the form of process mapping and guidance notes where required.

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 Aqua DNA consists of a download and export of data held, in an agreed format, and removal of hardware from site. 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

Data import formats

Data import formats

- CSV
- Other

Other data import formats

JSON

Analytics

Metrics

Service usage metrics

Yes

Metrics types

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

Reporting types

- Real-time dashboards
- Reports on request

Resource tagging

No

FOCUS resource tagging

No

Scaling

Independence of resources

A dedicated level of support is agreed with customers during the proposal phase and this is detailed within the scope. All clients are hosted in separate databases and servers are continually monitored to ensure that resource levels are adequate.

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

No

Security governance approach

Jacobs takes all aspects of security very seriously and we provide the top level of service support. Hosted solutions provided by Jacobs Digital have undergone regular penetration testing by an independent 3rd party security consultancy. Our SaaS (Software as a Service) platforms are available as fully managed hosted solutions on the internet, or we also offer heightened security hosting options including hosting within our client's network and bespoke secure network solutions.

Information security policies and processes

Jacobs offer integrated and truly secure enterprise- capable solutions that span the cybersecurity lifecycle. We are a market leader in cyber security offering the full breadth of security services. We offer a complete suite of cyber capabilities that range from holistic enterprise lifecycle security and secure business transformation, to threat assessment, risk management, security architecture, audit, review & penetrating testing, SOC and incident response (CIR). Because our services are engineered to align with the cybersecurity standards of our clients and market regulations (from the National Institute of Standards and Technology (NIST) to the Office of Nuclear Regulation and Ministry of Defence), the client is completely free choose the engagement model and service level that aligns with their needs. In particular, the Jacobs Cybernet secure network solution has been certified for use up to UK Official Sensitive and the highest Defence Cyber Protection Partnership level (usually reserved only for Secret). We also have a number of certified Secret networks across the UK.

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

In the event of an incident the Aqua DNA Service Support Desk system will be the first point of contact. They will go through a pre-defined check list and determine if they can resolve the issue, if not they will contact the technical support team to follow up with the user. For a serious issue, such as a prolonged server outage, the Aqua DNA disaster plan will come in effect. After the incident is resolved a downtime post-mortem will be carried out to establish the exact cause and what can be done in future to avoid a repeat situation.

Staff security

Staff security clearance

Staff screening performed but doesn't conform with BS7858:2019

Government security clearance

Up to Security Clearance (SC)

Secure development

Approach to secure software development best practice

Conforms to a recognised standard, but self-assessed

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

Aqua DNA has an admin interface accessed by the Jacobs support desk 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