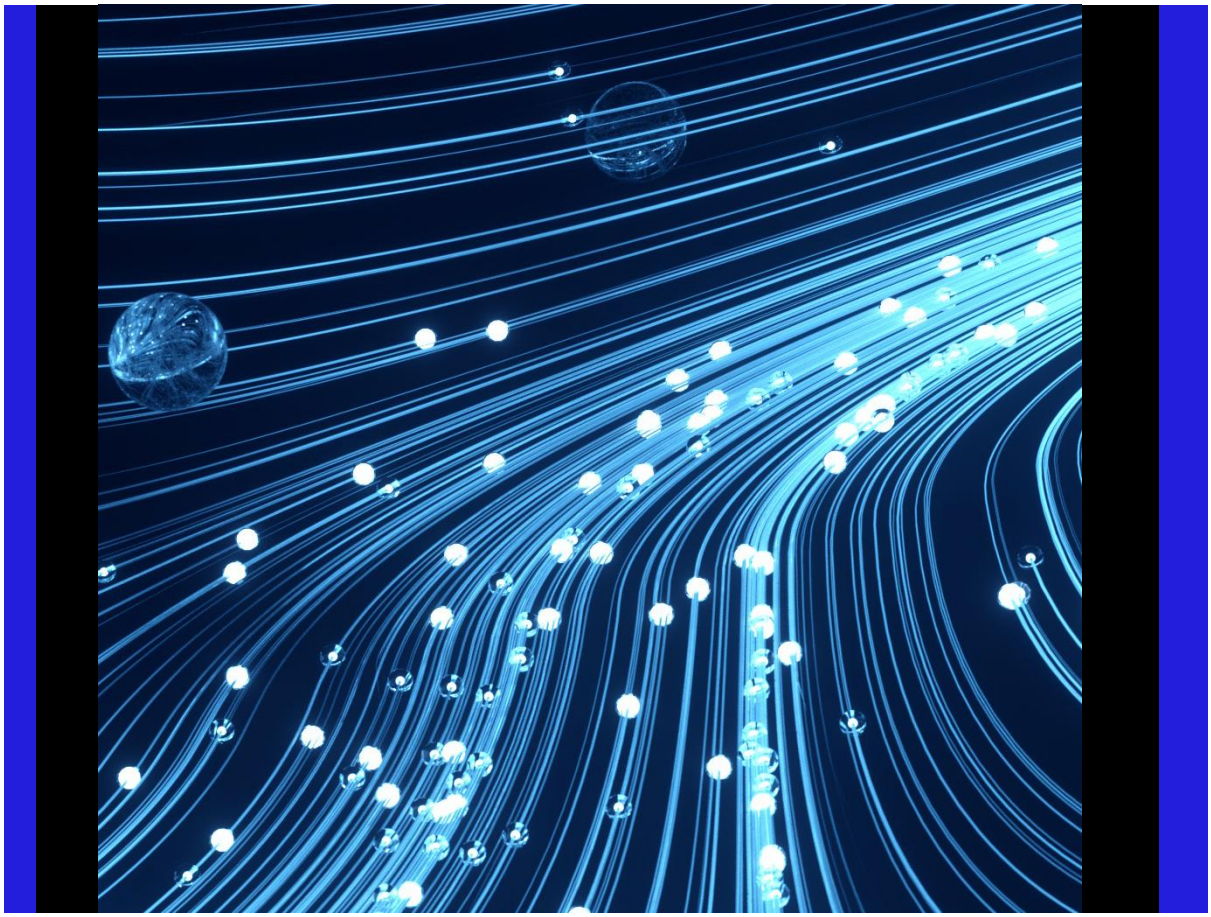
Jacobs

Service Definition Document – Flood Platform

Document no: 001
Revision: v1.0

CCS - G-Cloud 15
19 January 2026



Service Definition Document – Flood Platform

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_FloodPlatform

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

Service type

Lot 2b: Software as a Service (SaaS)

Service name

Service name

Flood Platform

About your service

Service description

Flood Platform is a cloud-based solution designed to unify and streamline flood modelling workflows. It provides a centralised hub for model management, enabling secure storage and collaboration among modelling teams and stakeholders. Includes advanced visualisation tools for modelling data and results, simulation and analysis capabilities, and integrated reporting features.

Service categories

- Application Development and Deployment
  - Analytics and business intelligence
    - Location and geospatial data management and analytics
      - Location and geospatial data management and analytics

Multi cloud support

No

Service features and benefits

Service features and benefits

Service features

- Secure centralised model storage and version control
- Cloud-based storage, simulation and analysis of flood data
- Visulationsation tools, clear, actionable insights
- Automated generation of compliance-ready reports
- Granular role-based access controls

- Real-time sharing across teams and organisations
- Automated workflows. Standardised processes to streamline operations
- External data integration capability
- QA review and validation tools
- Future-ready AI enhancements

Service benefits

- Centralised model storage and management - ensures access and sharing
- Cloud-Based Simulation – Run simulations quickly with scalable resources
- Visualisation Intuitive visual tools for clear insights
- Automate report generation to reduce errors and improve compliance
- Collaboration Tools – realtime feedback across teams and organisation
- Enterprise-grade security with two-factor authentication protects data.
- Standardise processes to boost efficiency and reduce operational costs.
- Seamlessly connect with external sources for richer analysis.
- QA – Perform collaborative QA checks to accelerate delivery.
- AI - Future ready enhancements driven by AI

Service scope

Add-ons and extensions

Software add-on or extension

No

Cloud deployment model

Public cloud

Service constraints

No

System requirements

- Compliant web browser
- Internet connection
- 3rd party software licences where applicable (extended functionality) e.g. TUFLOW

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

Response within 1 working day. Standard support not provided during weekends or UK Public Holidays. Enterprise support available 7 days a week.

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

No

Support levels

User support is provided via a dedicated knowledge base and a technical support team, with tickets created online, via email or phone call. Our support SLA is detailed here https://app.floodplatform.com/page/support-policy Cost of support is included in service subscription fee Enhanced support available on request at additional cost Support engineers accessed via front line support

Support available to third parties

No

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

No

User support

User support accessibility

WCAG 2.2 A

API

API

No

Customisation

Customisation available

No

Onboarding and offboarding

Getting started

An onboarding session is available at start of all new contracts - delivered online. In-built step-through guides assist new users. Knowledge base includes quick start guides

Documentation

Service documentation

Yes

Documentation formats

HTML

Documentation accessibility standard

WCAG 2.2 A

End-of-contract data extraction

Customers (users) are able to self download the data at any point to their desktop. We provide a grace period at the end of the contract to enable download. If a customer requires data transferring to another cloud location or service provider (e.g. Azure Blob Storage) this can be arranged (may attract an additional cost).

End-of-contract process

Access to the operational features of the platform and support ceases. Users ability to store additional data, undertake data processing or simulations also ceases. Users have a grace period to download their data. If a customer requires data transferring to another cloud location or service provider (e.g. Azure Blob Storage) this can be arranged (may attract an additional cost).

Data importing and exporting

Data export approach

There is a "Export" function that enables users to to download partial or full flood model data files (input and output). There is also the ability to "Transfer" data to another organisation.

Data export formats

Data export formats

Other

Other data export formats

Native model data file formats

Data import formats

Data import formats

Other

Other data import formats

- Native model data file formats.
- Non-model data - PDF, Microsoft office, etc

Analytics

Metrics

Service usage metrics

Yes

Metrics types

Data Storage used, Data Processing Compute Credits used, Simulation Credits used. These are provided at Organisational, Teamspace, and Project level.

Reporting types

Real-time dashboards

Resource tagging

No

FOCUS resource tagging

No

Scaling

Independence of resources

We are able to auto-scale workloads, specifically core functionality, data processing and simulations. However, compute resources (quota) for simulations (CPU and GPU) are constrained by the limits (quota) placed upon us by Microsoft. On request we can arrange with Microsoft for additional quota.

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

- Private network or public sector network
- TLS (Version 1.2 or above)

Protection within your network

Data protection within supplier network

- TLS (Version 1.2 or above)
- Other

Other protection within supplier network

Kubernetes Ingress controller

Asset protection

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

- United Kingdom
- Other locations

User control over data storage and processing locations

No

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 every 6 months

Penetration testing approach

In-house

Protection of data at rest

Protecting data at rest

- Physical access control, complying with CSA CCM v4.0
- Encryption of all physical media

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

- Deleted data can't be directly accessed / Cryptographic Erasure
- Data Erasure

Equipment disposal approach

Complying with a recognised standard, for example CSA CCM v4.0, CAS (Sanitisation) or ISO/IEC 27001

Availability and resilience

Guaranteed availability

Jacobs shall, subject to paragraph 2.6 of our support policy (https://app.floodplatform.com/page/support-policy), use Commercially Reasonable Efforts to make Flood Platform available twenty-four hours a day, seven days a week, except for when planned and unscheduled maintenance need to be carried out. Both planned and unscheduled maintenance will be undertaken at times to cause the least disruption and with as much advance notice as possible. DATA RESILIANCE Data resilience is based on Microsoft Azure Locally Redundant Storage (LRS): LRS stores three copies of your data that all reside within a single data centre. The data is written across all three copies synchronously. LRS storage provides a resiliency of 11 nines (99.999999999 %) over a given year. While LRS storage protects your data from drive or server rack failures, the availability of data would be impacted if an outage ever affects the data centre used to host Flood Platform.

Approach to resilience

It's available on request.

Outage reporting

Users will be notified of planned outages in advance via email. Users are notified of outages in progress (both planned and unplanned) via the service login page.

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

All service components, including application code, configuration, and infrastructure, are version-controlled and tracked using Azure DevOps. Each change is linked to a work item, providing traceability through to deployment. changes are reviewed and approved before development. Changes are assessed for security impact, including effects on data handling, access control, integrations, system exposure. Changes are developed in controlled environments and subject to peer review and automated checks. The service is penetration tested by internal IT prior to deployment to production. Any identified issues must be resolved before release. Only approved are deployed using auditable release processes. Only approved individuals can deploy.

Vulnerability management type

Supplier-defined controls

Vulnerability management approach

Potential threats are assessed through a combination of automated tooling and internal security review. This includes static code analysis, automated dependency scanning, and regular security scans. The service is hosted on Azure, benefiting from platform monitoring Via Defender. Remediation actions are prioritised based on severity and potential impact. Patches and fixes are normally deployed as part of the regular development cycle, with releases occurring at least once per sprint (typically every two weeks). Where critical or high-risk vulnerabilities are identified, urgent hotfixes can be developed. All remediation activity is tracked and auditable.

Protective monitoring type

Supplier-defined controls

Protective monitoring approach

Azure hosting provides platform monitoring and threat detection, including security alerts from Defender. Application and infrastructure logs are captured and reviewed as part of operational support and incident investigation. Security alerts and findings from automated tools or internal IT security scans are reviewed and acted upon as required, with remediation tracked through established change and vulnerability management processes. Remediation actions are prioritised based on severity and potential impact. Patches are deployed as part of the regular development cycle, with releases occurring at least once per sprint. Where critical or high-risk vulnerabilities are identified, hotfixes can be developed.

Incident management type

Supplier-defined controls

Post-quantum cryptography secure

No

Incident management approach

Pre-defined processes are in place for common event types, including service outages, security issues, and platform-related incidents. These processes define assessment, response, escalation, and resolution activities. Users report incidents by submitting a support ticket or by emailing the Flood Platform support team. All incidents are logged, assessed for severity and impact, and tracked through to resolution. Where relevant, incidents are communicated to users via email. Communications are proportionate to the nature and impact of the incident and may include status updates and resolution information. Incident outcomes are recorded and used to inform service improvements and preventative actions.

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

Supplier-defined process

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

Users permissions are assigned and managed by organisations. Only organisation "owners" and "admins" can access restricted interfaces. There are no restrictions on access to support channels.

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 have access to real-time 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 have access to real-time 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

Yes

Free or trial versions

Free trial available

Yes

Description of free trial

14 Day Free access Basic onboarding No support via telephone Support via email Limited free credit for data analysis and simulation

Link to free trial

www.floodplatform.com