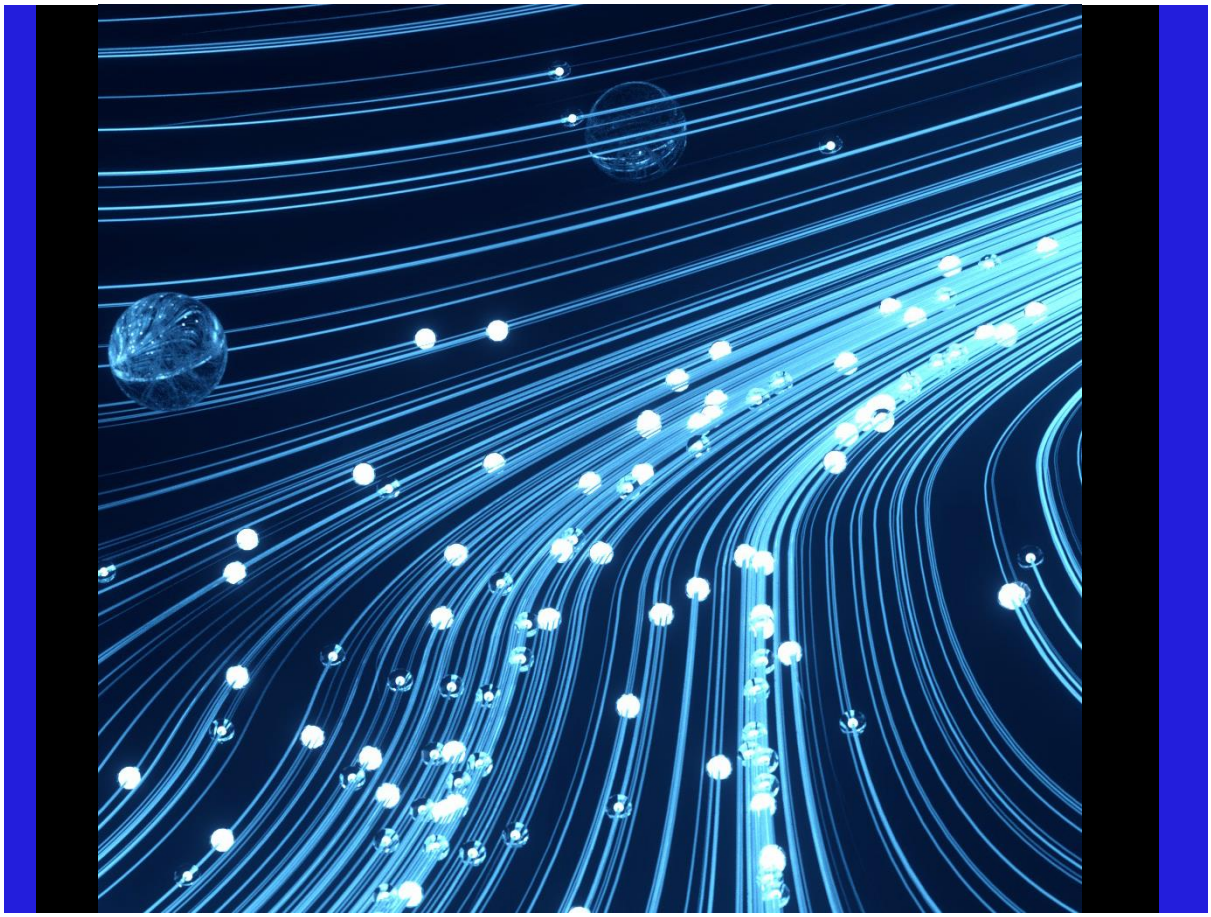
Jacobs

Service Definition Document – Track Record Engage

Document no: 001
Revision: v1.0

CCS - G-Cloud 15
19 January 2026



Service Definition Document – Track Record Engage

Client name:	n/a		
Project name:	CCS - G-Cloud 15		
Client reference:	Jacobs	**Project no:**	n/a
Document no:	001	**Project manager:**	Hugh McMichael
Revision:	v1.0	**Prepared by:**	Jamie Kelley
Date:	19 January 2026	**File name:**	Dragonfly G-Cloud 15 ServiceDef

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

Dragonfly

About your service

Service description

Web-based, cloud hosted AI/ML/computer vision solution to process sewer pipe inspection CCTV video and automatically detect, identify and code pipe defects to determine pipe condition. 100% QC of model outputs. Includes an integrated asset management module providing reliable business intelligence, optimises sewer reinspection, maintenance schedules, rehabilitation and optimises asset performance.

Service categories

- Applications
  - Engineering
    - Computer-Aided Engineering Applications
      - Computer-Aided Engineering Applications
    - Collaborative product data management
      - Collaborative product data management

Multi cloud support

No

Service features and benefits

Service features and benefits

Service features

- Condition assessment of gravity sewer pipes using AI
- Identification of defects in sewer pipes from CCTV inspection videos
- Coding identified sewer defects to industry standards

- Coded defect results output for use in customer CMMS
- Integrated asset management module analyses coded defect results output
- Asset management recommendations (pipe repair, rehabilitation, replacement and inspection schedule)

Service benefits

- Consistent, accurate, and fast coding of sewer pipe defects
- High quality inspections, insights, and decision-making
- Increased process productivity and efficiency
- Save 30-40% in sewer defect coding time
- O&M and capital costs savings
- Improved labour/talent management
- Efficient and proactive asset management and investment decisions

Service scope

Add-ons and extensions

Software add-on or extension

No

Cloud deployment model

Public cloud

Service constraints

Service requires pipe metadata and CCTV inspection video for sewer to be condition assessed to be uploaded by the client into Dragonfly for condition assessment.

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

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

SLAs to be agreed with client on a case-by-case basis.

Support available to third parties

Yes

How users work with your service

Browsers

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Chrome

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 - email is used for first line support.

Accessibility standards

None or don't know

Description of accessibility

Service interface is via email.

Accessibility testing

No testing undertaken with users of assistive technology yet.

User support

User support accessibility

None or don't know

API

API

No

Customisation

Customisation available

No

Onboarding and offboarding

Getting started

Training and support is provided with uploading sewer CCTV video inspection files and populating pipe metadata template with associated pipe data.

Documentation

Service documentation

Yes

Documentation formats

- PDF
- Other

Other documentation formats

mp4

Documentation accessibility standard

None or don't know

How the documentation is accessible

Provided to client in onboarding email.

End-of-contract data extraction

Data is downloaded by the client.

End-of-contract process

Data is downloaded by the client prior to the end of the contract. There are no additional demobilisation tasks required and no additional charges.

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

PDF

Data import formats

Data import formats

Other

Other data import formats

- mp4
- mpg
- avi
- wmv
- Jacobs-provided metadata inventory template (Excel)

Analytics

Metrics

Service usage metrics

No

Scaling

Independence of resources

A dedicated level of support is agreed with customers during the proposal phase which is detailed within the scope of work. 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

Other locations

User control over data storage and processing locations

No

Datacentre security standards

Managed by a third party

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

Other

Other data at rest protection approach

Dragonfly provides data integrity and protection with its use of Azure Blob Storage, which provides for a fast, highly reliable, and persistent file storage for our application in the cloud. Blob storge is optimised for storing massive amounts of data and is designed for: serving images and documents directly to a browser, storing files for distributed access, streaming video and audio, storing data for backup and restore, disaster recovery, and archiving.

Data sanitisation process

Data sanitisation process

No

Equipment disposal approach

In-house destruction process

Availability and resilience

Guaranteed availability

SLA's 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

Username or password

Access restrictions in management interfaces and support channels

Dragonfly 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).

Access restriction testing frequency

At least every 6 months

Management access

Management access authentication

Username or password

Audit information for users

Audit for buyers' users' actions

Access to user activity audit information

No audit information available

Audit for suppliers' users' actions

Access to supplier activity audit information

No audit information available

How long system logs are stored for

At least 12 months

Pricing

Discount for educational organisations

No

Free or trial versions

Free trial available

Yes

Description of free trial

Jacobs offers limited free trials for potential clients.