

Service Definition: Secure AI & Data, DevOps, Cloud Security

This document provides a detailed technical overview of the **Secure AI & Data, DevOps, Cloud Security** platform, a fully managed Software as a Service (SaaS) solution designed for the UK public sector.

1. Service Scope and Capabilities

The platform provides a standardized environment for the entire AI and software development lifecycle. It is designed to extend existing **Lot 1 Cloud Hosting** and **Lot 2 Enterprise Software** with advanced analytical and automation layers.

- **AI Lifecycle Management:** Tools for data labelling, AI model building, and MLOps foundation model operations.
 - **Advanced AI Services:** Standardized modules for Generative AI, Computer Vision, Document AI, and Anomaly Detection.
 - **DevOps Automation:** Pre-configured pipelines for secure application development and deployment across AWS and Azure.
-

2. Technical Requirements and Access

To ensure optimal performance and security, buyers must meet the following standardized requirements:

- **Browser Access:** Access via modern web browsers (Chrome, Edge, Firefox, or Safari).
 - **Connectivity:** A stable internet connection with minimum 10Mbps upload/download speeds.
 - **Identity Management:** Support for SAML 2.0 or OpenID Connect for secure single sign-on (SSO).
 - **Cloud Integration:** Authorized API keys and administrative access to existing AWS or Azure environments.
-

3. Security and Resilience

The platform is architected according to the government's **2nd cloud security principle: 'Asset protection and resilience'**.

- **Resilience:** Geographically redundant datacentre zones with automated failover and real-time data replication.
 - **Protective Monitoring:** 24/7 automated log analysis and real-time security event monitoring.
 - **Vulnerability Management:** Continuous automated scanning and critical patching deployed within 24–48 hours of validation.
 - **Information Security:** Policies overseen by a dedicated Head of Information Security reporting to the Board.
-

4. Service Management and Support

We provide a structured approach to ensure high availability and user success.

- **Availability Guarantee:** Target 99.9% uptime during core business hours, supported by service credits for failures.
 - **Outage Reporting:** Real-time visibility via a public dashboard, status API, and automated email alerts.
 - **Incident Management:** Pre-defined processes for common events with root-cause analysis reports provided post-resolution.
 - **Onboarding:** Searchable documentation, setup guides, and self-paced online training modules.
-

5. Data Ownership and Contract End

Buyers retain full ownership of their data throughout the contract lifecycle.

- **Data Extraction:** Self-service downloads (CSV, JSON), bulk API retrieval, or secure file transfer.
- **Purging:** Secure data destruction in accordance with G-Cloud standards following successful extraction confirmation.
- **Pricing:** Standard extraction assistance is included; bespoke migration support may incur additional costs.