

Terms and Conditions Summary: Secure AI & Data, DevOps, Cloud Security

This summary outlines the core contractual obligations and protections for the Secure AI & Data, DevOps, Cloud Security SaaS platform, ensuring alignment with G-Cloud framework standards.

1. Service Level Agreement (SLA) and Credits

Uptime Commitment: We provide a guaranteed service availability of 99.9% during core business hours.

Service Credits: If availability falls below the guaranteed threshold, buyers are eligible for service credits calculated as a percentage of the monthly subscription fee.

Maintenance Windows: Scheduled maintenance is excluded from uptime calculations, with users notified at least 48 hours in advance.

2. Data Protection and Security

Data Ownership: The buyer retains exclusive ownership of all data ingested, processed, or generated within the platform.

Information Security Policies: All data processing complies with robust security policies overseen by a dedicated Head of Information Security.

Access Control: Management interfaces are restricted via multi-factor authentication (MFA) and role-based access controls (RBAC).

Audit Rights: We maintain continuous auditing and monitoring processes to ensure ongoing compliance with UK data protection legislation.

3. Usage Restrictions and API Limits

Acceptable Use: Users must not attempt to modify the underlying multi-tenant infrastructure or bypass global security policies.

API Constraints: While the API allows for extensive automation, bulk data exports are subject to rate-limiting to maintain platform stability for all users.

Intellectual Property: Use of the platform does not grant the buyer ownership of the underlying software, AI modules, or proprietary DevOps code.

4. Responsibilities of the Buyer

System Requirements: The buyer is responsible for ensuring their environment meets the minimum technical specifications, including browser compatibility and internet bandwidth.

Account Security: Buyers must manage their own administrative access rights and protect API keys used for AWS/Azure integrations.

Compliance: The buyer must ensure their use of AI and data processing meets internal organizational policies and legal requirements.

5. Termination and Data Extraction

Contract End: Upon termination, the platform provides standardized self-service or assisted paths for data extraction.

Data Purging: Following a confirmed successful extraction, we perform a secure purge of all buyer data in accordance with G-Cloud security standards.

Exit Assistance: Basic extraction support is included in the contract price, while bespoke migration services are subject to additional fees.