

Service Definition: Millersoft Managed Apache Superset Service (iSaaS)

1. Service Overview

Millersoft provides a managed Apache Superset service delivering secure deployment, configuration, operation, and support of the open-source data visualisation and analytics platform. The service is designed for use on UK Government-aligned cloud infrastructure and is suitable for OFFICIAL and OFFICIAL-SENSITIVE workloads, subject to customer assurance and platform controls.

Apache Superset enables users to explore, analyse, and visualise data through interactive dashboards and charts without managing the underlying platform.

2. Scope of Service

The managed service includes: - Architecture design and deployment of Apache Superset - Secure configuration and platform hardening - Integration with approved data sources - Monitoring, alerting, and incident management - Patch and vulnerability management - Backup and configuration management - Change and release management - User support and service management

3. Supported Deployment Models

- Deployment on government-aligned cloud infrastructure
- Containerised or VM-based deployment models as agreed
- Private network access with restricted management interfaces

4. Security and Compliance

Millersoft applies supplier-defined security controls aligned with UK Government Cloud Security Principles.

4.1 Identity and Access Management

- Role-based access control within Superset
- Least-privilege access for users and administrators
- Strong authentication and MFA where supported

4.2 Network and Data Security

- TLS encryption for data in transit
- Private network deployment and IP restrictions
- No permanent storage of source data within Superset

4.3 Vulnerability Management

- Monitoring of Apache Superset security advisories and CVE feeds
- Timely deployment of patches and updates

- Mitigating controls where immediate patching is not possible

4.4 Protective Monitoring

- Centralised logging and monitoring of application and access events
- Alerting on anomalous behaviour or service degradation

5. Service Management

5.1 Incident Management

- Supplier-defined incident management process
- Severity-based prioritisation and response
- Incident reporting and post-incident reviews

5.2 Change and Configuration Management

- Controlled change process with impact and security assessment
- Planned maintenance windows and customer notification

6. Support Model

- Standard support (9x5) included
- Optional enhanced support (24x7)
- Named support contacts and regular service reviews

7. Customer Responsibilities

Customers are responsible for: - Providing and managing underlying data sources - Data quality, classification, and governance - User access requests and role approvals

8. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including export of dashboards, metadata, and configuration
- Secure service decommissioning

9. Service Levels

Service availability targets, response times, and service credits are defined contractually and documented separately.

10. Exit and Portability

- Use of open standards and export tools
- Support for service exit and knowledge transfer
- Assistance with migration to successor services where agreed