

Service Definition: Millersoft Managed MongoDB Service (iSaaS)

1. Service Overview

Millersoft provides a managed MongoDB database service delivering secure deployment, configuration, operation, and support of the MongoDB document-oriented database on government-aligned infrastructure. The service is designed for deployment on UK public sector environments and supports scalable, flexible data models for modern digital services.

2. Licensing and Open Source Position

MongoDB Community Edition is licensed under the **Server Side Public License (SSPL)**. Millersoft provides MongoDB as a managed service in accordance with the terms of the SSPL. Millersoft does not redistribute MongoDB software for standalone use and does not restrict customer access to their data. Customers retain full ownership of their data at all times. Licensing implications are explained transparently as part of procurement and onboarding.

3. Scope of Service

The managed service includes: - Architecture design and deployment of MongoDB databases and replica sets - Secure configuration and database hardening - High availability configuration using replica sets - Monitoring, alerting, and incident management - Backup, restore, and recovery support - Patch and vulnerability management - Change and release management - User support and service management

4. Supported Deployment Models

- Government-aligned public or private cloud environments
- On-premise or virtual machine deployments
- Private network access with restricted administrative interfaces

5. Security and Compliance

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

5.1 Identity and Access Management

- Role-based access control using MongoDB roles
- Least-privilege access for users and administrators
- Secure authentication mechanisms

5.2 Network and Data Security

- TLS encryption for data in transit
- Network segmentation and firewall controls

- Secure handling of credentials and secrets

5.3 Vulnerability Management

- Monitoring of MongoDB security advisories and CVE feeds
- Timely deployment of security patches
- Mitigating controls where immediate patching is not possible

5.4 Protective Monitoring

- Centralised logging of database, system, and access events
- Alerting on anomalous behaviour and service degradation

6. Service Management

6.1 Incident Management

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

6.2 Change and Configuration Management

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

7. Support Model

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

8. Customer Responsibilities

Customers are responsible for: - Application design and database usage patterns - Data classification, retention, and governance - User access requests and role approvals

9. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including data export and configuration handover
- Secure service decommissioning

10. Service Levels

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

11. Exit and Portability

- Support for logical database export and migration

- Use of standard MongoDB tools and formats
- Knowledge transfer to the customer or successor supplier