Service Definition: Millersoft Managed ClickHouse Service (iSaaS)

1. Service Overview

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

ClickHouse enables high-performance analytical queries on large datasets, supporting real-time and batch analytics use cases.

2. Scope of Service

The managed service includes: - Architecture design and deployment of ClickHouse clusters - Secure configuration and platform hardening - Replication and high-availability configuration where required - Monitoring, alerting, and incident management - Backup and data recovery configuration - Patch and vulnerability management - Change and release management - User support and service management

3. Supported Deployment Models

- Government-aligned public or private cloud environments
- On-premise, virtual machine, or bare-metal deployments
- Kubernetes-based deployments where appropriate
- Private network access with restricted administrative 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 using ClickHouse users and roles
- Least-privilege access for users and administrators
- Integration with customer authentication mechanisms where supported

4.2 Network and Data Security

- TLS encryption for data in transit
- Network segmentation and firewall controls
- Secure handling of credentials and secrets

4.3 Vulnerability Management

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

4.4 Protective Monitoring

- Centralised logging of database, system, and access events
- Alerting on anomalous behaviour, errors, and performance issues

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 security and impact 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: - Data ingestion, schema design, and query logic - Data classification, retention, and governance decisions - User access requests and role approvals

8. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including data export and configuration handover
- 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 SQL-based interfaces
- Support for data export, replication, or migration

• Knowledge transfer to the customer or successor supplier