Service Definition: Millersoft Managed OpenSearch Service (iSaaS)

1. Service Overview

Millersoft provides a managed OpenSearch service delivering secure deployment, configuration, operation, and support of the open-source OpenSearch search and analytics platform. 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.

OpenSearch provides scalable search, log analytics, and data exploration using open standards and an Apache 2.0 licence.

2. Scope of Service

The managed service includes: - Architecture design and deployment of OpenSearch clusters - Secure configuration and platform hardening - Integration with applications, log sources, and data pipelines - Monitoring, alerting, and incident management - Patch and vulnerability management - Backup and snapshot configuration - 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 using supported tooling
- 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 (RBAC)
- Least-privilege access for users and administrators
- Integration with customer authentication providers where supported

4.2 Network and Data Security

- TLS encryption for data in transit
- Encrypted storage and snapshots where supported
- Network segmentation and IP allow-listing

4.3 Vulnerability Management

- Monitoring of OpenSearch security advisories and CVE feeds

- Timely deployment of security patches
- Mitigating controls where immediate patching is not possible

4.4 Protective Monitoring

- Centralised logging of cluster, system, and access events
- Alerting on anomalous behaviour and 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 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: - Providing and managing indexed data and log sources - Data classification, retention, and governance - User access requests and role approvals

8. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including export of indices, snapshots, 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 APIs
- Support for data export and migration
- Knowledge transfer to the customer or successor supplier