Service Definition: Millersoft Managed Kubernetes Service (iSaaS)

1. Service Overview

Millersoft provides a managed Kubernetes service delivering secure deployment, configuration, operation, and support of Kubernetes container orchestration platforms. The service is designed for deployment on UK Government-aligned cloud or on-premise infrastructure and supports the reliable operation of containerised applications and microservices.

The service removes the operational complexity of running Kubernetes while enabling customers to benefit from scalable, resilient, and portable application platforms.

2. Scope of Service

The managed service includes: - Architecture design and deployment of Kubernetes clusters - Secure cluster configuration and hardening - Configuration of networking, ingress, and storage integration - Monitoring, logging, and alerting - Patch and vulnerability management - Backup and recovery of cluster 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
- Single or multi-node Kubernetes clusters
- 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 identity providers where supported

4.2 Network and Data Security

- Network segmentation and Kubernetes network policies
- TLS encryption for control plane and API access
- Secure handling of secrets and credentials

4.3 Vulnerability Management

- Monitoring of Kubernetes and component 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 cluster, node, and access events
- Alerting on anomalous behaviour, failures, and resource exhaustion

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: - Container images, application code, and deployment manifests - Data classification, retention, and governance - User access requests and workload configuration

8. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including cluster configuration export
- 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 Kubernetes APIs
- Support for workload migration and configuration export
- Knowledge transfer to the customer or successor supplier