Service Definition: Millersoft Managed RabbitMQ Service (iSaaS)

1. Service Overview

Millersoft provides a managed RabbitMQ service delivering secure deployment, configuration, operation, and support of the open-source RabbitMQ message broker. 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.

RabbitMQ enables reliable, asynchronous messaging between systems, supporting event-driven and decoupled architectures.

2. Scope of Service

The managed service includes: - Architecture design and deployment of RabbitMQ clusters - Secure configuration and platform hardening - Configuration of queues, exchanges, and routing patterns - Monitoring, alerting, and incident management - Patch and vulnerability management - Backup of configuration data - 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 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 using virtual hosts and permissions
- 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
- Network segmentation and IP allow-listing
- Secure management interfaces

4.3 Vulnerability Management

- Monitoring of RabbitMQ 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 broker, cluster, 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: - Application design and message handling logic - Data classification and retention decisions - User access requests and role approvals

8. Onboarding and Offboarding

- Structured onboarding with documentation and walkthroughs
- Offboarding support including queue draining and 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 protocols and standards
- Support for message draining and configuration export
- Knowledge transfer to the customer or successor supplier