Service Definition: Millersoft Managed Apache Kafka Service (iSaaS)

1. Service Overview

Millersoft provides a managed, bespoke Apache Kafka service designed for deployment on UK Government-aligned cloud infrastructure. The service supports Apache Kafka deployments on either bare metal infrastructure or Kubernetes (K8s), depending on customer requirements. The service is suitable for OFFICIAL and OFFICIAL-SENSITIVE workloads, subject to customer assurance and platform controls.

Apache Kafka provides a distributed event streaming platform for high-throughput, low-latency data pipelines, event-driven applications, and operational analytics.

2. Scope of Service

The managed service covers: - Architecture and design of Kafka clusters - Installation and configuration of Kafka (and supporting components as agreed) - Deployment on bare metal or Kubernetes - Secure configuration and hardening - Ongoing operational management - Monitoring, alerting, and incident response - Patch and vulnerability management - Backup and recovery configuration support - Support and service management

3. Supported Deployment Models

3.1 Bare Metal Deployment

- Dedicated physical hosts or virtualised infrastructure
- OS hardening aligned with CIS or equivalent benchmarks
- Isolated network segments
- Storage and capacity configured for throughput and retention requirements

3.2 Kubernetes Deployment

- Helm or manifest-based deployments
- Kubernetes-native networking, storage, and secrets management
- Horizontal scaling using Kubernetes primitives
- Rolling upgrades and automated restarts where appropriate

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 and least privilege
- Strong authentication and MFA for administrative access where supported

- Separation of duties between operational roles

4.2 Network Security

- Private network deployment and segmentation
- Encrypted communications using TLS (in-transit encryption)
- Restricted management access via VPN/private network or IP allow-listing

4.3 Vulnerability Management

- Monitoring of upstream Kafka security advisories and CVE feeds
- Dependency vulnerability monitoring for supporting components
- Timely deployment of security patches
- Mitigating controls applied where immediate patching is not possible

4.4 Protective Monitoring

- Centralised logging of system and service events
- Monitoring of broker health, replication, controller events, and client access
- Alerting on anomalous behaviour and policy violations
- Incident triage and investigation

5. Service Management

5.1 Incident Management

- Supplier-defined incident management process
- Incident classification by severity and impact
- Rapid response to high-severity incidents
- Root cause analysis and corrective actions

5.2 Change and Release Management

- Controlled change process for configuration and upgrades
- Planned maintenance windows
- Testing in non-production where applicable
- Rollback procedures where feasible

5.3 Backup and Recovery

- Configuration of backup processes for cluster configuration and metadata (as applicable)
- Support for customer-defined retention, snapshotting, and restore testing

6. Support Model

- Named support contacts and agreed support channels
- Incident reporting via email and/or secure support portal
- Defined response and resolution targets
- Regular service reviews covering availability, incidents, and capacity

7. Customer Responsibilities

Customers are responsible for: - Providing underlying infrastructure and cloud platform unless otherwise agreed - Data classification and handling decisions - Network connectivity and perimeter controls - Client/application configuration and producer/consumer logic

8. Assumptions and Dependencies

- Apache Kafka is provided under an open-source licence
- The service does not include application development unless explicitly agreed
- Accreditation depends on the customer platform, operating model, and shared responsibility

9. Exit and Portability

- Assistance with service termination
- Export of configuration and operational runbooks
- Support for data migration and topic export where in scope
- Knowledge transfer to customer or successor supplier

10. Service Availability

Service availability targets and maintenance arrangements are agreed contractually and documented separately.

11. Service Levels (SLAs and SLOs)

Unless otherwise agreed, the following targets apply.

11.1 Availability SLO

- Target service availability: **99.5% per calendar month** (excluding planned maintenance)
- Availability applies to core Kafka broker service and agreed supporting components

11.2 Incident Response SLAs

Incidents are prioritised by severity and impact:

- **Severity 1 (Critical):** Service unavailable or major data pipeline disruption
- Response target: **1 hour**
- Ongoing updates: At least every **4 hours** until resolution
- **Severity 2 (High):** Significant degradation with no workaround
- Response target: **4 hours**
- **Severity 3 (Medium):** Limited impact or workaround available
- Response target: **1 business day**

• **Severity 4 (Low):** Minor issue or service request

• Response target: **2 business days**

11.3 Resolution Targets (SLOs)

• Severity 1: Restore service as soon as practicable, target **within 1 business day**
• Severity 2: Target **within 3 business days**
• Severity 3: Target **within 10 business days** or via planned change

11.4 Planned Maintenance

• Planned maintenance is scheduled in advance and notified to customers
• Maintenance windows are excluded from availability calculations

11.5 Service Reporting

• Regular service reviews may include availability, incidents, and performance metrics
• SLA performance is reviewed jointly with the customer

12. Service Credits and Penalties for SLA Failure

Where Millersoft fails to meet an agreed SLA, the customer may be entitled to service credits, subject to the terms below. Service credits are the customer's sole and exclusive remedy for SLA failures.

12.1 Availability Service Credits

If monthly availability falls below the agreed SLA (excluding planned maintenance and customer-caused issues), the following service credits apply: - **≥ 99.0% and < 99.5%:** 5% of the monthly service charge
- **≥ 98.0% and < 99.0%:** 10% of the monthly service charge
- **< 98.0%:** 20% of the monthly service charge

12.2 Incident Response SLA Credits

If response targets for Severity 1 or Severity 2 incidents are missed, Millersoft may apply a service credit of up to **5% of the monthly service charge per incident**.

12.3 Credit Cap

Total service credits in any calendar month are capped at **20% of the monthly service charge**. Service credits are applied as a future invoice adjustment and are not redeemable for cash.

12.4 Exclusions

Service credits do not apply where SLA failure results from: - Customer actions or omissions - Failures of customer-provided or third-party infrastructure - Force majeure events - Emergency security actions taken to protect the service

12.5 Continuous Improvement

Repeated SLA failures trigger a service review and corrective action plan to prevent recurrence.