

CMS Application – Service Definition

Version number: 1.0.0
Document Date: 26/01/2026
Document classification: Public



Contents

CMS Application – Service Definition	1
Executive Summary	1
Solution Architecture & Hosting.....	1
Hosting Environment	1
Security Standards	2
Functional Capabilities	3
Support Service Definition	4
Scope of Support.....	4
Out of Support Scope	4
Incident Management	4
Service Requests	4
User Guidance & “How-to” Support.....	5
Incident Prioritisation & SLA.....	5
Maintenance & Patching Management.....	6
Onboarding & Implementation	7
Exclusions & Limitations	7
Document Control	9
Version Control	9
Next Review Date	9
Contact Details	9
Distribution	9

Executive Summary

Tribal provides a fully managed, cloud-hosted CMS designed to centralise and streamline interactions with stakeholders. Our solution offers a secure, accessible, and intuitive platform for managing customer records, case histories, and workflow automation.

By leveraging a highly secure cloud infrastructure, we ensure that sensitive customer data is protected with enterprise-grade encryption and rigorous access controls. The platform removes the administrative burden from your team by automating routine tasks and providing a "single source of truth" for all customer interactions. As a fully managed service, Tribal handles all underlying maintenance, security patching, and data backups, ensuring your team has 24/7 access to a compliant and reliable system.

Solution Architecture & Hosting

Hosting Environment

- **Infrastructure:** The CMS platform is hosted within Microsoft Azure's UK based cloud platform to ensure high levels of resilience, performance and compliance with UK data protection laws.

Key characteristics include:

- Cloud Infrastructure: Multi-tier architecture deployed within Azure, benefiting from Microsoft's enterprise grade resiliency, security framework and global availability.
- Data Sovereignty: All application, database, and backup data resides exclusively within UK Azure regions. No data leaves the UK at any stage unless contractually agreed.
- Availability: Service availability SLA of 99.9%, measured monthly, excluding planned maintenance windows.
- Backup & Disaster Recovery:
 - Daily full backups and hourly transaction log backups – air gapped from the system.
 - 30-day retention as standard.
 - RTO 24 hours / RPO 24 hours, with options to enhance these for organisations requiring higher resilience.

A DR environment is maintained in line with the hosting provider's capabilities, allowing restoration of service in the event of a platform failure, data corruption or catastrophic incident.

Security Standards

- **SSL/TLS:** All communication between clients, services, and backend components is encrypted in transit using modern Transport Layer Security (TLS) protocols. The platform enforces TLS 1.2 as a minimum baseline, with full support for TLS 1.3 where available. This ensures robust protection against eavesdropping, man-in-the-middle (MITM) attacks, and traffic tampering. Cipher suites are aligned with industry best practice, and deprecated or insecure protocols are disabled by default.
- **WAF:** A Web Application Firewall (WAF) is deployed at the network edge to provide an additional defensive layer for public-facing endpoints. The WAF is configured to detect and block malicious traffic patterns, including those identified within the OWASP Top 10 (e.g., injection attacks, cross-site scripting, broken access control, and request forgery). Continuous rule updates and threat intelligence feeds ensure the environment benefits from up-to-date signatures and behavioural protections.
- **Authentication:** Authentication and access control are aligned with modern Zero Trust principles. Provider Core integrates directly with Azure Active Directory to support secure, centralised identity management. The platform enables:
 - **Multi Factor Authentication (MFA):** Enforced to mitigate credential compromise by validating user identity through multiple verification methods.
 - **Single Sign-On (SSO):** Simplified and secure access to the platform using Azure AD authentication tokens, reducing password fatigue and improving overall user experience.
 - **Conditional Access Policies:** (Optional but recommended) Organisations can apply Azure AD conditional access policies to govern access based on device compliance, user risk level, geolocation, and other contextual signals.

Functional Capabilities

The CMS platform offers a broad range of configurable features to support frontline delivery teams, case management processes, and operational oversight: Complete end-to-end

Core Features

- End-to-end configurable case management with workflow automation.
- Graphical contract builder with deadlines, triggers, and scheduled actions.
- Survey/assessment builder with version control.
- Action Plans with intelligent recommendations.
- Integrated diary management with Outlook synchronisation.
- Multi-channel communications (SMS, email, letter templates, call logging).
- User-customisable dashboards, widgets and real-time reporting tools.
- PRaP integration for pipeline and referral management.
- GDPR-aligned auditing, redaction tools, and right-to-erasure workflows.
- CRM and vacancy management for employment-related services.

Key Benefits

- Intuitive User Experience accelerates user adoption and training.
- Build flexible contracts with context-aware deadlines and automation
- Graphical participant journeys provide status, clarity and next-step visibility
- Build and share Dashboards to keep advisors informed of priorities
- Clear diary management for Team Leaders, advisors and participants
- Survey designer captures structured, actionable participant feedback
- Automated communications keep your participants informed.
- Transparency with in-screen user auditing throughout.
- Secure data in an ISO27001 accredited environment, hosted within Azure

Support Service Definition

- **Hours:** Monday – Thursday 08:00 – 17:30; Friday 08:00 – 16:30 (excluding bank holidays).
- **Channels:** Web Portal, Email, and Telephone.

Scope of Support

Tribal provides comprehensive support designed to ensure the stability, security and usability of the CMS platform.

Out of Support Scope

Platform enhancements, bespoke configuration & development of features, however these can be implemented at additional costs.

Incident Management

Some examples of what would be considered an incident.

- **System Availability:** Resolution of outages or connectivity issues preventing access to the CMS.
- **Data Integrity:** Investigation of record save failures, data sync errors, or duplicate entry issues.
- **Logic & Workflow Failures:** Troubleshooting automated processes that fail to trigger (e.g., "The email alert didn't send when the case was closed").
- **Reporting Errors:** Diagnosing issues where reports or dashboards fail to generate or display incorrect data sets.
- **Performance:** Investigation of slow search queries or record load times.

Service Requests

Some examples of what would be considered a service request.

- **User Provisioning:** Creation/deletion of staff accounts and resetting MFA tokens.
- **Permission Changes:** Modifying user access levels (e.g., granting a user access to 'Sensitive' case files).
- **Data Imports/Exports:** Assistance with bulk importing data (via CSV/Excel) or extracting data for external audits.
- **Field Configuration:** Minor adjustments to drop-down list options or field labels (where supported by the configuration UI).
- **Audit Requests:** Generating security logs to track user activity for compliance purposes.

User Guidance & “How-to” Support

- **Workflow Advice:** Guidance on how to best structure a case or workflow within the system.
- **Search Assistance:** Helping users construct complex search queries to find specific customer segments.
- **Feature Explanation:** "How-to" support for standard system functions (e.g., "How do I merge two duplicate customer records?").

Incident Prioritisation & SLA

Priority Level	Description (Specific to CMS Application)
Major Incident	Any incident that carries significant operational, regulatory or reputational risk and therefore requires heightened focus, accelerated response, and coordinated end-to-end incident management. Major Incidents typically require senior technical oversight, proactive communication to stakeholders, and may involve invocation of Business Continuity or Disaster Recovery processes.
P1 – Critical Impact	A platform-wide or service-critical failure that results in total loss of access to the CMS for all users or prevents delivery of critical frontline services. Examples include complete service outage, data corruption affecting live operations, failure of authentication systems (e.g., Azure AD outage), or critical workflow engines failing system-wide. This priority applies where customer operations cannot proceed and immediate restoration is required.
P2 – High Impact	A significant functional issue affecting a large proportion of users or a core feature essential to service delivery. Examples include major reporting failures, workflow automation halting for entire departments, persistent system performance degradation, or communications module failure (SMS/email) impacting time-sensitive contractual notifications. The system remains accessible, but important functionality is impaired.
P3 – Standard Impact	A non-critical issue affecting a subset of users or a specific module, where a workaround exists and core operations continue. Examples include errors affecting a specific contract configuration, intermittent dashboard failures, incorrect data rendering in non-critical reports, or issues isolated to a single team/site. These issues require resolution but do not materially impact service continuity.
P4 – Low Impact	Minor issues with limited impact on day-to-day operations. Examples include isolated display issues, non-urgent configuration adjustments, minor UI/UX defects, or functional queries requiring investigation but not affecting delivery. These are typically service requests or low-severity defects that can be scheduled for routine resolution.

Priority	Impact	Response Time	Resolution Time	Communication Frequency	Service Level Objective
1	Critical	1 hour	4 hours	Every hour	95%
2	High	2 hours	6 hours	Every 2 hours	95%
3	Standard	4 hours	12 hours	Every 4 hours	90%
4	Low	8 hours	24 hours	Every 8 hours	85%

Maintenance & Patching Management

- CMS Core Updates:** The CMS platform is actively maintained to ensure ongoing security, stability and compatibility. All critical and high-severity patches released by the CMS vendor are assessed upon availability and scheduled for deployment within 14 days. This includes security fixes, performance improvements, and updates required to maintain compliance with UK public-sector security guidance.

Updates are deployed during planned maintenance windows to minimise disruption, and all releases undergo regression testing prior to roll-out to ensure service continuity.

- Plugin/Module Updates:**
 The system incorporates a number of approved third-party plugins and modular extensions to support enhanced functionality. These components are continuously monitored, and any critical or high-severity vendor updates are reviewed within 14 days of release.
- Where updates are necessary to address security vulnerabilities or functional defects, they are integrated into the platform in line with our controlled release process. Lower-severity enhancements or optional module updates are bundled into scheduled maintenance cycles to reduce change frequency for end users.
- Browser Compatibility:** To ensure a consistent, secure and accessible user experience, the CMS application is tested and supported on the latest two major versions of the following web browsers:
 - Microsoft Edge
 - Google Chrome
 - Mozilla Firefox
 - Apple Safari
- Pen Testing:** The platform undergoes annual penetration testing, conducted using a combination of internal and independent third-party independent check

accredited security specialists. These tests evaluate the application, API endpoints, authentication mechanisms and infrastructure controls against recognised industry standards (e.g., OWASP Testing Framework).

Testing includes:

- External black box assessments
- Internal authenticated testing
- Vulnerability scanning
- Validation of remediation actions

Findings are risk assessed and tracked through to closure, ensuring the CMS remains robust, compliant and aligned to UK Government cyber security expectations. Additional tests may be commissioned following major architectural changes or emerging threat intelligence.

Onboarding & Implementation

- **Provisioning:** Standard setup of the production is 21 days, however bespoke configuration may increase the setup time based on requirements.
- **Training:** 2 x remote “train the trainer” sessions and access to Knowledge Base.

Exclusions & Limitations

The following items fall outside the scope of the standard service fee and are **not included** as part of the core CMS SaaS offering. These activities may be provided as additional, chargeable services under a separate Statement of Work (SoW) or Call-Off Contract where required.

Custom Development

The standard service includes access to the out-of-the-box CMS features and configuration options. Any requirement to extend system functionality through **new** code development, bespoke modules, custom API endpoints, or feature enhancements not currently part of the product roadmap is outside of scope.

Where organisations require functionality that is unique to their service model, these changes can be delivered through paid consultancy or development engagements, subject to feasibility assessment and commercial approval.

Custom Report Development

Whilst the CMS includes standard reports, dashboards, and configurable data views, the creation of **complex bespoke SQL reports**, custom aggregations, cross-system analytics, or Business Intelligence (BI) dashboards (e.g., Power BI, Tableau) is not included in the standard support service.

Customers requiring specialist reporting solutions, tailored KPIs, contractual

performance visualisations, or integration into external BI platforms may commission these as a separate professional service.

Data Cleansing

The responsibility for ensuring that legacy or source data is accurate, complete and suitably prepared for migration lies with the customer.

This includes:

- Removing duplicate records
- Correcting data quality issues
- Standardising formats
- Validating field values
- Addressing missing or corrupted information

Although data import templates and guidance are provided, the manual cleansing and preparation of datasets remain the Client's responsibility.

Migration of Existing Data

The standard onboarding service provides import templates and guidance but does **not** include the end-to-end migration of a client's historical data from existing systems.

Customers are responsible for:

- Extracting data from legacy platforms
- Transforming data to meet CMS import specifications
- Ensuring source data is validated, accurate and complete

Tribal can assist by providing documentation, optional consultancy, and quality checks, but the labour and ownership of the migration process itself sit with the Client unless contracted separately.

Legacy Browser Support

The CMS is optimised for modern, secure web browsers and supports only the latest two major releases of Edge, Chrome, Firefox and Safari.

Fixes, compatibility testing, or troubleshooting for:

- Outdated browser versions
- Unsupported operating systems
- Deprecated web technologies

are not included within standard support. Customers are responsible for ensuring their environment meets the minimum technical requirements to access the service.

Document Control

This is the change history and sign off information.

Version Control

Record of Amendment		
Version Number	Date of Issue	Detail of Change
V1.0	26/01/2026	LD – Technical Architect - Initial version

Next Review Date

The next scheduled review of this document will be 26/01/2027

Contact Details

Author:	Lee Dudmish – Technical Architect
Approver:	Nathan Churchman – Head of IT Services

Distribution

Distribution:	All Tribal Colleagues & Public Entities