Service Definition

Webcurl Self-Service Portal

1. Service Overview

The Webcurl Self-Service Portal provides a configurable, cloud-hosted interface that enables citizens, staff, and partners to submit forms, create cases, upload documents, and interact securely with Dynamics 365, Power Platform and Dataverse. The service enhances automation, reduces manual processing, and improves user experience through a modern, accessible portal aligned with public-sector standards.

2. Key Features

- Customisable forms, journeys, and workflows
- Secure integration with Dynamics 365 and Dataverse
- Document upload and case creation
- Role-based access and authentication options
- Optional integration with GOV.UK Pay and other APIs
- Responsive, WCAG-compliant user interface
- Power Platform automation support
- Usage metrics via Microsoft cloud tools (Power BI, Application Insights, Dataverse analytics)

3. Onboarding & Configuration

Webcurl configures the portal to meet customer requirements, including form design, branding, data mapping, workflow integration, and testing. Customers may extend functionality using Power Platform tools.

4. Service Levels & Availability

Webcurl guarantees **99.9% availability** for the portal layer when hosted in Webcurl-managed Azure. This is underpinned by Microsoft's SLAs for Azure and Dynamics 365/Dataverse. Service credits apply if availability falls below guaranteed levels.

5. Resilience & Datacentre Architecture

The service benefits from Azure's resilient, geographically distributed datacentres, redundant compute and storage, automated failover, and continuous replication. Detailed architecture is available on request.

6. Outage Reporting

Outages are communicated through Webcurl's service desk with email alerts to nominated contacts. Microsoft provides public dashboards and APIs for underlying platform status. Customers hosting in their own Azure environment may configure their own alerts.

7. Information Security

Webcurl maintains policies covering access control, secure development, incident response, vulnerability management, and data protection. Policies align with industry standards and Microsoft cloud security controls. Privileged access is tightly restricted, logged, and periodically reviewed.

8. Configuration & Change Management

All components are tracked through a configuration register. Changes are logged, risk-assessed for security impact, tested, approved, and deployed through controlled processes with rollback capability.

9. Vulnerability Management

Threats are identified through continuous monitoring, automated scanning, and threat-intelligence feeds (Microsoft advisories, CVEs, industry bulletins). Critical vulnerabilities are patched as quickly as practicable; others follow scheduled maintenance windows.

10. Protective Monitoring

Azure and Dynamics 365 logs, alerts, and anomaly detection identify potential compromises. High-severity incidents trigger immediate investigation, containment, and remediation. All incidents follow a structured response process.

11. Incident Management

Predefined processes cover common events. Users report incidents via the service desk. Webcurl provides incident reports summarising impact, root cause, and corrective actions. Major incidents include follow-up reporting.

12. Access Control for Management & Support

Administrative access uses named accounts, MFA, least-privilege roles, and audited logs. Customer environments are accessed only with explicit approval. All support interactions are recorded for traceability.

13. Trial Version

A time-limited demonstration portal is available for evaluation. It includes sample forms and navigation but excludes customer configuration, integrations, data storage, support, SLAs, and production use.