



GCloud15 - Service Definition

myVCU – Victim Services Case Management System

Connektivity

1. Services Overview

Services Description

myVCU is a secure, cloud-based (SaaS) victim care case management system designed to support the delivery of victim services across single or multi-agency environments. The platform enables organisations to manage victim referrals and cases from initial intake and triage through to support delivery, risk assessment, support plans, outcomes tracking, and case closure.

myVCU provides a centralised system for managing victim data, referrals, tasks, documentation, communications, and reporting within one secure platform. It supports collaboration between police, commissioned providers, and voluntary sector organisations while ensuring that sensitive victim information is protected through robust security and access controls.

The service is designed to reduce administrative burden, improve oversight and consistency, and enable victim services teams to focus on delivering timely, coordinated, and victim-centred support.

Services Outcomes

myVCU supports improved victim care delivery by providing:

- A single, authoritative view of victim referrals and cases
- Secure and controlled information sharing across partner agencies
- Faster referral triage and allocation
- Improved monitoring of service delivery and outcomes
- Enhanced compliance with victim care standards and reporting requirements

The service enables commissioners and service leads to maintain operational oversight while supporting frontline practitioners with efficient, intuitive tools.

Target Customers

myVCU is designed for UK public sector and third-sector organisations involved in the delivery, coordination, or commissioning of victim services, including:

- Police forces
- Police & Crime Commissioners (PCCs)
- Central Victim Care Units (VCUs)
- Commissioned voluntary and community sector providers
- Multi-agency victim services partnerships

The service supports both single-organisation use and complex, multi-agency operating models.

Service Context and Operating Model

Victim care services frequently operate across multiple organisations, requiring secure information sharing, clear accountability, and consistent processes. myVCU is designed to operate as a central coordination platform, supporting:

- External and internal referral intake
- Referral triage and case assignment
- Victim intake, needs assessment, and risk indicators
- Ongoing case management and communication
- Signposting and support tracking
- Outcome measurement and reporting

Role-based access controls ensure that users only access information appropriate to their role and organisation, supporting confidentiality while enabling effective collaboration.

Key Benefits

- Reduced administrative workload through centralisation and automation
- Improved visibility of victim journeys and service delivery
- Faster and more secure referral handling
- Enhanced multi-agency collaboration
- Improved data quality and reporting accuracy
- Scalable to regional or national victim service models
- Secure handling of OFFICIAL and OFFICIAL-Sensitive data
- UK-hosted cloud service aligned with public sector security expectations

Key Differentiators

- **Victim-centred design**
Purpose-built to support victim services, referrals, and care pathways rather than generic case or incident management.
- **Multi-agency referral and triage model**
Supports secure referrals from multiple organisations, centralised triage, and controlled onward allocation to accredited providers.
- **Granular role-based access controls**
Multiple user access levels ensure that sensitive victim data is only visible to authorised users, supporting confidentiality and information-sharing obligations.
- **Secure external referral capability**
Enables partner agencies to submit referrals securely and, where required, track referral progress without exposing full case records.

- Outcome and service effectiveness tracking
Built-in tools to record outcomes, victim feedback, and service impact, supporting commissioning oversight and statutory reporting.
- Designed for UK public sector use
UK-hosted SaaS platform aligned to OFFICIAL and OFFICIAL-Sensitive data handling requirements and public sector security standards.
- Configurable without bespoke development
Configurable fields, workflows, reports, and access models allow services to adapt the platform to local operating models without code changes.
- Scalable deployment models
Supports single-organisation, regional, or multi-tenant victim care unit models, with optional dedicated tenant deployments.

2. Features and Functions

This section describes the functional capabilities of the myVCU service, outlining the core features available to users and the technical capabilities that support delivery of restorative justice services at scale. The features are designed to support end-to-end case management, multi-agency collaboration, and robust reporting while maintaining strong security controls.

Core Features

- Centralised victim and case management
- Secure referral intake and triage workflows
- Risk Assessment and Support Plans
- Multi-agency case collaboration
- Role-based user access controls
- Configurable fields and workflows
- Task and deadline management
- Secure document storage and management
- Victim needs and risk indicators
- Case status and lifecycle tracking
- Outcome and signposting recording

Reporting and Data Management

- Standard and configurable reports
- Export of data to Excel for further analysis
- Support for statutory and stakeholder reporting requirements
- Data export to Data Warehouse

Technical Capabilities

- Web-based access (no client-side installation required)
- SaaS delivery model hosted in the UK
- Secure HTTPS access
- Role-based access control and audit logging
- Data export in common formats (e.g. Excel)
- Configurable data fields and lookup values
- API-enabled system integration (subject to scope and agreement)
- Integration options discussed on a case-by-case basis

3. Service Delivery Model

This section explains how the myVCU service is delivered, deployed, and operated. It outlines the cloud deployment approach, onboarding and setup activities, and the division of responsibilities between the supplier and the customer during live service operation.

Deployment Model

- Public cloud Software as a Service (SaaS)
- Hosted in UK-based data centres
- Multi-tenant architecture with logical separation of customer data
- Private Cloud available on request (with extra hosting costs)

Onboarding and Setup

The onboarding process may include (some elements chargeable):

- Technical discussions with customer IT teams
- System configuration and tenant setup
- Customisation of fields, workflows, and user roles
- Data migration from legacy systems
- User and administrator training

Each customer is assigned a product consultant during onboarding to support initial setup and adoption.

Operational Model

- Platform maintenance, updates, and security managed by the supplier
- Customers manage users, access roles, and operational use of the system
- Regular updates delivered as part of the SaaS service

4. Service Levels and Performance

This section sets out the service availability targets, support coverage, and incident response commitments associated with the myVCU service. These measures are designed to provide customers with confidence in service reliability, performance, and operational support.

Availability

- Target service availability: 99.9% (excluding planned maintenance)
- Service is designed to be available 24x7

Planned maintenance is notified in advance where possible.

Support Coverage

- Support hours: 08:00–18:00 UK time, Monday to Friday (excluding UK bank holidays)
- Support channels: email and telephone
- Optional enhanced or out-of-hours support available by agreement

Incident Response Targets

Priority	Description	Initial Response	Investigation Start
P1 – Critical	Production system unavailable	1 hour	1 hour
P2 – Serious	Major functionality impaired	2 hours	4 hours
P3 – Moderate/Low	Minor issue or workaround available	2 hours	8 hours

5. Security, Compliance and Assurance

This section summarises the security controls, compliance standards, and assurance measures that underpin the myVCU service. It is intended to demonstrate how the service supports public sector security and data protection requirements.

Security Standards and Certifications

- ISO/IEC 27001 (Information Security Management)
- ISO 9001 (Quality Management)
- Cyber Essentials Plus
- IASME Governance
- ICO registered data controller

Data Protection and Residency

- All customer data hosted within the UK
- Designed to support OFFICIAL and OFFICIAL-Sensitive data
- Physical separation of customer tenants available (at additional cost)

Encryption and Access Control

- Encryption in transit using HTTPS
- Encryption at rest, including encrypted database fields
- Role-based access controls
- Two-factor authentication (2FA) for user access

Backup and Resilience

- Daily backups with 28-day retention
- Secure backup storage within UK data centres
- Resilience provided through accredited hosting infrastructure

6. Support and Escalation

This section describes the support arrangements for the myVCU service, including how customers can raise issues, how incidents are prioritised, and the escalation process used to ensure timely resolution.

Support Model

This section describes how customers access support services, the hours during which support is available, the communication channels offered, and how support requests are prioritised and managed.

Support coverage is provided during standard business hours: - Support hours: 08:00 to 18:00 UK time -
Support days: Monday to Friday, excluding UK public holidays

Customers can contact the support team via: - Telephone - Email

All support requests are logged and assessed on receipt. Issues are graded based on severity and business impact, ensuring that critical incidents affecting service availability or core functionality are prioritised appropriately. Lower-impact issues are managed in line with agreed response targets.

Extended or enhanced support coverage outside of standard hours, including evenings, weekends, or public holidays, can be provided by prior agreement and may be subject to additional charges.

Escalation Process

This section explains how support issues are escalated within the supplier organisation to ensure appropriate visibility and timely resolution.

- Initial triage by service desk
- Escalation to senior technical support where required
- Escalation to Support Manager based on severity or time to fix
- Management escalation for critical or prolonged incidents

Customers are kept informed throughout incident resolution.

7. Exit Management and Offboarding

This section explains how customers can exit the myVCU service at the end of a contract or upon termination. It covers data extraction, secure data deletion, and the support available to ensure an orderly and compliant transition away from the service.

Exit Support

This section describes the support available to customers when exiting the service, including assistance with data extraction and transition planning. At contract end or upon termination, customers can request support for service exit, which may include:

- Export of customer data in a commonly used electronic format (e.g. Excel)
- Secure transfer of exported data to the customer
- Consultancy around the export and structure of data (additional charge)

Data Deletion

This section explains how customer data is securely removed from the service following exit, in line with data protection and security requirements.

- Customer data is securely deleted following confirmation of successful data export
- Data deletion is performed in accordance with data protection and security policies
- Certificate of destruction can be issued if required

Timescales

This section outlines the typical timescales associated with exit activities, subject to agreement based on data volume and complexity. Data export requests are typically fulfilled within an agreed timescale, depending on data volume and complexity. Data exports are typically undertaken at weekends or outside of core work hours.

Charges

This section clarifies which exit-related activities are included within the service and which may incur additional charges.

- Standard data export is included, if extra data exports are required this will incur additional costs
- Additional exit support or bespoke assistance may be chargeable by agreement