

Service Definition: Public Sector Access, Data, AI and Integration Services

Service overview

This service provides design, implementation and advisory support to help public sector organisations improve access, reduce demand, strengthen data integration, and adopt AI safely. It combines digital access design, workflow automation, data and integration services, and AI governance to support policing, healthcare, mental health and wider public services.

The service supports improved visibility, reduced contact volumes, better coordination and more effective use of data and automation without replacing existing core systems.

Service scope

The service includes discovery, assessment, design, configuration, integration, implementation and advisory support. It covers digital front doors and contact reduction, data and system integration, intelligence enablement, AI governance and assurance, and data platform strategy and delivery. The service does not include operational decision-making or clinical advice.

Supported service use cases

This service definition supports the following service offerings: - Police Data, Integration and Intelligence Enablement - Public Sector Digital Front Door and Contact Reduction - Public Sector AI Governance and Ethical AI Advisory - Salesforce Data Cloud Strategy and Implementation (Public Sector) - Mental Health Digital Access and Engagement

Users

The service supports authorised public sector staff, partner organisations and service users where appropriate. Access is restricted using role-based access controls and strong authentication.

Service components

- Digital access and contact reduction design
- Workflow and process automation
- Data integration and system connectivity
- Reporting, dashboards and operational insight
- AI governance, assurance and operating model design
- Salesforce and MuleSoft implementation services
- Secure cloud-based delivery

Support and service levels

Support is provided during UK business hours with priority-based response and resolution targets. Managed support options are available, including access to a support portal, dedicated service management and regular service reviews.

Onboarding and offboarding

Onboarding includes service setup, access provisioning, integration configuration and knowledge transfer. Offboarding includes secure removal of access, data handling in line with contractual requirements and service closure activities.

Security and compliance

The service operates within an ISO/IEC 27001 certified Information Security Management System and is supported by Cyber Essentials Plus. Controls include access management, monitoring, incident management and change control. Underlying platform security is provided by cloud service providers where applicable.

Resilience and availability

The service uses resilient cloud platforms with built-in redundancy and monitoring. Operational processes support incident management, service continuity and customer communication.

Data handling

Data is processed and stored in accordance with contractual and public sector data protection requirements. Access to data is restricted, logged and auditable.

Change management

Changes are managed through a controlled change management process, including impact and security assessment, testing and controlled deployment.

Service boundaries

The service does not provide clinical diagnosis, treatment decisions, legal advice or autonomous decision-making. Responsibility for operational decisions remains with the customer.