

Secure User Account and Role-Based Portal Platforms

Service Definition

1. Service overview

Secure User Account and Role-Based Portal Platforms is a design and development service for creating digital portals with user accounts and role-based access controls. The service supports public sector organisations that need controlled, secure access to services, information and workflows based on defined user roles and permissions.

2. How the service works

The service is delivered through a structured design and build process focused on secure access management.

Typical delivery activities include:

- Onboarding to confirm objectives, scope, users and constraints
- Analysis of user types, roles and permission requirements
- Design of role-based access models and account structures
- Definition of user journeys and access-controlled workflows
- Portal interface design
- Front-end portal development
- Back-end application development and configuration
- Implementation of authentication and authorisation mechanisms
- Integration with existing systems where required
- Accessibility-informed build and validation
- Pre-release testing and issue resolution

The buyer provides access to stakeholders, documentation and systems required for delivery. Delivery is typically remote.

3. Skills and experience

The service is delivered by a multidisciplinary team experienced in secure portal and access-controlled platform development.

Roles typically involved include:

- Delivery or project manager
- Business analyst
- UX designer
- Front-end developer
- Back-end developer
- Quality Control
- Solutions Architect

The team applies established user-centred design and secure development practices appropriate to public sector digital services.

4. Relevant experience

The supplier has the ability to deliver secure, role-based portals for public sector and regulated organisations.

- User portals with account registration and permissions management
- Role-based platforms supporting different access levels and responsibilities
- Secure portals integrated with existing internal or third-party systems

Operational platforms that support controlled access and improved service management.

5. Onboarding and offboarding

Onboarding

The service begins with mobilisation to confirm scope, timelines, stakeholders and access requirements. The buyer provides access to relevant users, documentation and systems needed for delivery.

Offboarding

Offboarding includes:

At completion, all developed portal code, documentation and agreed deliverables are handed over to the buyer. A handover session is used to explain the solution and operational considerations.

6. Service constraints

The service covers design and development only and does not include ongoing hosting, support or operational management. Delivery depends on timely buyer input, approvals and access to systems. Authentication methods and access models are limited to those agreed during delivery. Integrations are restricted to systems made available by the buyer and may require third-party approval. Significant legacy system changes are outside scope.

7. Service management and support

Delivery is managed by a named delivery lead responsible for coordination, progress reporting and communication. Regular updates are provided during delivery. Risks and issues, including access and integration dependencies, are identified and escalated as required. Ongoing support after delivery is not included.

8. Technical and operational requirements (if applicable)

Buyer involvement may include providing access to identity systems, APIs, documentation and test environments. No specialist buyer-provided tools are required beyond agreed collaboration and review tools.

9. Hosting, data and security

Hosting is not included as part of this service. Buyer-provided data is used solely for delivery purposes and handled in line with agreed security and confidentiality requirements. The service does not include live data hosting, business continuity or disaster recovery arrangements.

10. Exit, data return and deletion

At the end of the service, all buyer-owned materials and developed assets are returned as part of the agreed handover. Any copies of buyer data held for delivery purposes are deleted in line with agreed confidentiality arrangements. No ongoing access or transition support is provided beyond handover activities.



HM Government
G-Cloud
Supplier

SPINDOGS