

Service Definition Document: Engeneum Online

Provider: Engeneum

Service Name: Secure Cloud Document Management & Workflow

Cloud Platform: Microsoft Azure

1. Service Overview

Engeneum provides a secure, cloud-native Document Management System (DMS) hosted on Microsoft Azure. The service enables the secure storage, rapid retrieval, and automated workflow processing of business-critical documentation.

Designed for the UK public sector, the platform replaces physical archives and disjointed file shares with a centralized, searchable digital repository. It ensures strict data sovereignty (UK-only data residency) and compliance with modern security standards.

2. Core Functional Modules

Module 1: Document Storage & Retrieval

A centralized repository for storing digital records with granular access controls.

- **Indexing & Search:** Documents are indexed via metadata and content (OCR), allowing users to retrieve records instantly using keyword searches.
- **Role-Based Access:** Access is restricted by department, role, or document type. Users only see the files they are explicitly authorized to access.
- **Audit Trails:** Every view, download, and modification is logged, providing a full audit history for compliance purposes.

Module 2: Invoice Processing & Approval Workflow

An automated workflow solution designed to streamline the accounts payable process.

- **Workflow Routing:** Invoices are automatically routed to the correct cost centre manager or budget holder for authorization based on pre-defined logic.
- **Approval Status:** Finance teams can track the status of any invoice in real-time (e.g., "Pending Approval," "Authorized," "Rejected"), reducing bottlenecks.
- **Integration:** Approved data can be exported to finance systems, reducing manual data entry errors.

Module 3: Secure ePayslips and HR Portal

A self-service portal allowing staff to access their payroll and HR documentation securely from any device.

- **Self-Service Access:** Employees log in via a secure web portal to view and download their own payslips and P60s, removing the need for printed distribution.
- **Historical Retention:** Users can access a full history of their pay documents (typically retained for 7+ years), reducing queries to HR/Payroll departments.
- **Security:** Personal financial data is protected by individual user credentials and Multi-Factor Authentication (MFA).
- **HR can determine which types of documents are available to the employee, the employee's manager or to HR only.**

3. Information Security & Protective Monitoring

The service utilizes Microsoft Defender for Cloud and Azure application gateway with WAF to provide continuous protective monitoring and threat detection across the infrastructure.

- **Threat Detection:** Real-time analysis of logs to identify misconfigurations, anomalies, and potential compromises.
- **Access Control:** Administrative and user access is governed by Azure Role-Based Access Control (RBAC). Multi-Factor Authentication (MFA) is enforced via Conditional Access policies for all external and administrative sessions.
- **Cryptographic Standards:** Data is encrypted in transit (TLS) and at rest (ADE).

4. Resilience & Availability

The service is architected for high availability using Microsoft Azure's UK regions.

- **Data Sovereignty:** Primary hosting in UK South, with a designated disaster recovery facility in UK West. All data remains strictly within the UK.
- **Availability:** The service targets a baseline availability of 99.9%.
- **Disaster Recovery:** Standard service includes automated daily backups and geo-redundant storage replication.
- **Enhanced Options:** A "Warm Standby" option is available for critical deployments, enabling rapid server failover to the secondary UK region in the event of a catastrophic primary site failure.

5. Support & Incident Management

Support is provided via a UK-based service desk. Incidents are prioritized and resolved according to the following Service Level Agreement (SLA) targets:

Stage	Target Time
Initial Response	Within 1 working hour
Begin Work	Within 4 working hours
Internal Escalation	After 4 working hours

6. Onboarding & Offboarding

- **Onboarding:** We follow a structured implementation plan including metadata definition, user permission mapping, and workflow configuration. Training is provided for administrators and end-users.
- **Offboarding:** At contract termination, all customer data can be deleted or extracted and returned in open, non-proprietary formats (e.g., PDF/TIFF for images, CSV/XML for metadata).