Service Definition: Data Security as a Service (DSaaS)

1. Executive Summary

Infotechtion's Data Security as a Service (DSaaS) delivers a fully managed, outcome-based solution to safeguard the UK Government's most sensitive data assets. Utilising the Microsoft Purview ecosystem, the service enables departments to transition from fragmented, manual data protection methods to a unified, automated, and proactive security posture.

Engineered to meet NCSC cloud security principles and public records management requirements, DSaaS ensures that digital estates remain secure and compliant with statutory obligations.

2. Service Overview

2.1 Purpose

To provide a scalable "Data Security as a Service" on the Microsoft Purview, Identity and Security platform, managing the complexity of data classification, protection, and lifecycle management. This allows public sector teams to operate within a "compliant by design" Microsoft environment.

2.2 Key Outcomes

- Automated Information Protection: classification and encryption of sensitive data (Official/Official-Sensitive).
- AI Readiness of Data: Ensuring departmental data is cleaned, classified, and correctly permissioned to enable the secure and effective rollout of Microsoft Copilot, Agents and generative AI technologies.
- Proactive Insider Risk Management: Detection of anomalous patterns to prevent data exfiltration.
- Regulatory Compliance: Automated retention and defensible disposition, aligned with UK GDPR and the Public Records Act (NI) 1923.
- Operational Agility: Managed feature backlog to ensure rapid adoption of new security innovations.

3. Addressing the Public Sector Skills Gap

The UK public sector currently faces a shortage of high-end Microsoft 365 security and information governance specialists.

Infotechtion DSaaS addresses this gap by offering "Expertise as a Service," removing recruitment burdens and providing immediate access to SC-cleared specialists with direct links to Microsoft Engineering. Departments are thus relieved from hiring niche operational governance roles.

3.1 Roles and Skills Provided

Role	Key Skills Provided
Purview Solutions Architect	Cross-tenant security design, technical roadmap orchestration, and architectural alignment with NCSC principles.
Information Governance SME	Expertise in records standards, statutory retention scheduling, and defensible disposition logic.
SecOps Analyst (Managed)	Threat hunting within Purview, Insider Risk triage, and correlation of security events within Microsoft Sentinel SIEM.
Compliance & Discovery Analyst	Advanced eDiscovery triaging for FOIs/SARs, policy tuning, and Compliance Manager score optimisation.
Learning & Adoption Specialist	Digital literacy assessment, micro-learning content creation, and persona-based communication strategies.

4. Service Features

- Automated classification of sensitive government data across all sources
- Real-time encryption for Official and Official-Sensitive information assets
- Continuous monitoring for unauthorised data sharing and exfiltration attempts
- Integration with NCSC cloud security and public records standards
- Proactive tracking of Microsoft Purview product roadmap and features
- Managed discovery of PII for Freedom of Information requests
- Automated retention policies based on statutory public record schedules
- SC-cleared expert support for all security and compliance operations
- Dynamic sensitivity labelling based on user context and location
- Unified dashboard for compliance posture and risk reduction reporting

5. Service Benefits

- Reduced risk of data breaches through automated protection controls
- Guaranteed compliance with UK GDPR and Public Records Act
- Faster response times for Subject Access and FOI requests
- Lower operational costs by automating manual data governance tasks
- Improved security posture aligned with NCSC best practices
- Seamless adoption of new cloud security innovations and tools
- Enhanced citizen trust through robust privacy and data safeguards
- Scalable governance that grows with departmental data requirements
- Expert guidance from security-cleared information management specialists
- Full visibility into data location and sensitive asset usage

6. Core Service Components (Service Catalogue)

The service catalogue serves a clear purpose for different teams within an organization to request standard services to improve their data posture and create a more business led approach to data posture management in addition to centralised IT , security and compliance initiatives.

Capability	**Description**
Data Security Posture	Autonomous scanning and indexing of data across M365, Azure, and legacy file shares to maintain a "Single View of Truth.", “single view of risks”, and a “single view of remediations” achieving a security posture score.
Information Protection	Design and management of Sensitivity Labels, automated watermarking, and persistent encryption.
Data Loss Prevention (DLP)	Monitoring and enforcement of policies to prevent unauthorised sharing of PII or sensitive departmental data.
Records Management	Implementation of automated retention schedules and disposition reviews.
eDiscovery & Audit	Managed support for FOI and SARs using Advanced eDiscovery.
Insider Risk & Privacy	Proactive monitoring of risky user activity and privacy risk assessments (Microsoft Priva).

7. Service Catalogue: Managed Activities

Service Area	**Activity (Performed by Infotechtion Resources)**

Governance & Roadmap	Roadmap Curation: Monthly review of Microsoft Message Centre and Public Roadmap to assess impact on Departmental configuration.
	Service Health Monitoring: Daily checks of Purview service health, connector status, and ingestion logs.
Data Security	Classifier Tuning: Continuous refinement of Sensitive Information Types (SITs) and Trainable Classifiers to improve detection accuracy.
	DLP Management: Proactive tuning of Data Loss Prevention policies to reduce "false positives" and optimise user prompts.
	Encryption Governance: Management of Sensitivity Label encryption rights and key rotation oversight.
Compliance Ops	Retention Orchestration: Updating and applying retention labels/policies as directed by Departmental Record Schedules.
	Disposition Triage: Preparation of monthly disposition reports and oversight of the technical deletion process once IAO approval is secured.
	eDiscovery Support: Technical search construction and triaging of content for SARs and FOI requests.
Risk & SecOps	Insider Risk Triage: Daily monitoring of high-severity alerts in the Insider Risk dashboard; escalating validated risks to SecOps.
	SIEM Integration: Maintaining the data feed between Purview logs and Microsoft Sentinel for cross-platform threat hunting.
Reporting & Quality	Posture Reporting: Monthly production of the Purview Compliance Scorecard and Risk Reduction KPI report.
	Learning Asset Creation: Production of technical user guides and micro-learning videos to support internal change initiatives.

8. Target Operating Model (TOM)

- Establishment of a governance framework integrated with existing IT and Security teams
- Demand Management: Standardised intake for new governance requirements
- Continuous Tuning: Monthly refinement of classifiers to reduce false positives
- Roadmap Curation: SMEs bridge to Microsoft Engineering, ensuring "Evergreen" security
- Service Reporting: Monthly Scorecard reporting on compliance posture and risk reduction KPIs

9. Business Change & Adoption (Supportive Model)

Our service enables existing departmental change initiatives, recognising that cultural change is internally driven:

- Provision of user guides, "How-to" videos, and micro-learning content tailored to departmental policies
- Persona-based educational assets for Compliance Managers, SecOps, IAOs, and End Users
- Adoption Insights: Reporting on label usage and policy overrides to target interventions
- Briefing Support: Technical expertise for internal town halls or stakeholder briefings

10. RAID: Risks, Assumptions, Issues, and Dependencies

Category	Description
Assumption	Operational Focus: Service is designed to operationalise and support implemented projects; not an implementation project service.
Assumption	Implementation Readiness: Assumes technical implementation projects are completed or underway; DSaaS provides the BAU framework.
Assumption	Change Ownership: Department owns the cultural change programme. Infotechtion provides supporting learning materials only.
Dependency	Licensing: Customer must maintain Microsoft 365 E5 or G5 licensing (or equivalent compliance add-ons).

Dependency	Administrative Access: Timely access to the customer's Microsoft 365 tenant with appropriate permissions is required.
Risk	Technical Debt: Initial implementation projects not following best practices may slow service throughput due to remedial configuration.
Risk	Roadmap Shift: Rapid changes to the Microsoft 365 roadmap may require unexpected policy adjustments outside standard monthly tuning.
Issue	Legacy Data Volatility: High volumes of ROT data in legacy areas may affect Data Map accuracy if not addressed by an implementation project.

11. Security, Sovereignty & Compliance

- Data Residency: All metadata and configuration remain within UK-based Azure regions (UK South / UK West)
- Security Clearance: All Infotechtion SMEs assigned to the service are SC cleared at minimum
- NCSC Alignment: Policies built against the 14 Cloud Security Principles
- Accessibility: Service interfaces and user guidance comply with WCAG 2.1 AA

12. Service Levels and Support (SLA)

Our support model is designed for high-availability public sector environments.

Priority	Impact	Response	Resolution
P1 - Critical	Total service loss / Material breach	20 Minutes	2 Hours (24/7)
P2 - High	Major disruption (25+ users)	20 Minutes	4 Hours (Business Hours)
P3 - Medium	Limited disruption	3 Hours	29 Hours
P4 - Low	Individual / Minor fault	7 Hours	44 Hours

Business Hours: Monday to Friday, 08:00 – 17:00 (Excluding NI/UK Bank Holidays)

13. Service Constraints

- Customers must maintain appropriate Microsoft 365 licensing to support Purview
- Support is focused on the Microsoft 365 cloud environment
- Physical disposition of paper-based records is not included
- Server-level patching or hardware maintenance is not included

- Running a full-scale standalone change programme is not included

14. Onboarding and Offboarding

14.1 Onboarding

- Readiness Audit: Assessment of implemented Purview configurations
- Catalogue Mapping: Definition of required service tiers for operational support
- TOM Integration: Alignment with departmental helpdesks

14.2 Offboarding (Exit Strategy)

- No vendor lock-in upon termination
- Handover of operational Purview configuration documentation
- Knowledge transfer of BAU tasks to internal staff

15. Pricing and Rate Card

The service is structured as a Monthly Subscription Fee. Additional project-based requirements (e.g., new implementations or legacy migrations) are serviced via a Standard Rate Card.

Refer to associated pricing document for a detailed breakdown of pricing options tailored to meet the needs of various public sector departments.

16. Why Infotechtion?

Infotechtion is uniquely positioned as a Microsoft Engineering Design Partner. Beyond implementation, we help build the tools themselves. Our expertise ensures UK Government departments successfully operationalise their security investments, attaining a mature security posture through expert managed oversight.