



Service Definition Document

Data Security
Enablement with
Microsoft Purview

Contents

Solution Overview.....	2
What is Data Security Enablement with Microsoft Purview?	2
Key Features.....	2
Key Benefits.....	2
Scope	3
What is in Scope?	3
What is Out of Scope?	4
Data Protection & GDPR.....	4
Why Partner with Atech?	5
Credentials and Capability	5
Microsoft Endorsements and Specialisations	5
Security and Compliance	6

Solution Overview

What is Data Security Enablement with Microsoft Purview?

Our Data Security Enablement service helps UK government organisations deploy Microsoft Purview to meet strict regulatory and security standards such as GDPR, NCSC guidance, and Public Sector compliance frameworks. Purview enables discovery, classification, and protection of sensitive data across all environments, ensuring robust governance, risk management, and policy enforcement.

Key Features

- Microsoft Purview deployment for unified data governance and compliance
- Automated data discovery across on-premises, cloud, and SaaS environments
- AI-powered classification and sensitivity labelling for structured/unstructured data
- Centralised compliance management and regulatory reporting capabilities
- Insider risk management and data movement monitoring tools
- Custom DLP policy design and implementation
- Retention policy configuration for regulatory and organisational requirements
- Integration with Office 365 and on-premises systems
- Optional deployment of AIP Scanner for on-premises data
- Continuous policy performance monitoring and optimisation

Key Benefits

- Enhanced compliance with GDPR, NCSC, and UK government standards
- Reduced risk of data breaches and insider threats
- Improved visibility and control over sensitive information
- Streamlined governance across hybrid and multi-cloud environments
- Stronger data security posture and organisational trust
- Simplified regulatory audits and reporting processes
- Consistent enforcement of retention and protection policies
- Lower complexity in managing data security and compliance
- Increased operational efficiency through automation and AI-driven insights
- Future-ready framework for evolving compliance and security requirements

Scope

What is in Scope?

Assessment

- Workshop to understand status, pain points and future requirements of DLP, Information Protection and Retention policies.
- Sensitive content discovery utilising content explorer and activity explorer.
- Output will be a report of current DLP and Information Protection configuration, sensitive content discovery and Retention Policies.
- Review and feedback workshop with system owner.

Design

- Define Sensitive info type and classification scheme.
- Define document storage locations for Office 365 and on-premises systems.
- DLP policy design.
- Information Protection design:
 - Sensitivity label design
 - Sensitivity label policy design.
- Retention policy design.
- Alerting design.
- Deployment roadmap.
- Review and feedback workshop with system owner.

Deployment

- Implement DLP policies.
- Implement sensitivity labels.
- Implement sensitivity label policies.
- (optional add-on:) Implement on-premises AIP Scanner for xx GB data.
- Implement Retention policies.
- Monitor policy performance and effectiveness.
- Review and update policies and procedures as needed.
- Review and feedback workshop with system owner.

Handover

- Deployment documentation produced and handed over to relevant team(s).
- Onboarding to managed services, if necessary.
- Handover to operational team.

What is Out of Scope?

- Working with users directly.
- Remediation of existing DLP policies.
- Remediation of existing sensitivity labels.
- Remediation of existing label policies.
- Data classification.
- Deployment of the virtual machines required for on-premises AIP scanning.
- Implementation of Microsoft Purview features/solutions not stated as in scope.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** – a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications



Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure



Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified**, **Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft’s top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.

ATECH IOMART

6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD