Flinders University have access to advance security and governance tools within the Microsoft 365 environment via their E/A5 agreement, specifically for this engagement the Microsoft Purview service.

Flinders University already has a data security policy with an agreed to and well published taxonomy - [Information Classification and Handling Procedures (flinders.edu.au)](https://www.flinders.edu.au/content/dam/documents/staff/policies/facilities-info-management/information-classification-handling-procedures.pdf)

Our eventual goal is

**Understand and govern our data** – Get greater visibility into all our data and manage assets across the environment

**Safeguard data where it lives –**secure our data throughout its lifecycle across apps, clouds and devices

**Improve risk and compliance posture –**Identify data risks and manage regulatory requirements

Currently the Microsoft 365 support team at Flinders do not have the required capabilities or capacity to complete the work listed in this service order. It is expected that the successfully panel member will complete all technical work on behalf of Flinders University and complete as built documentation to ensure handover can occur. We also request a short workshop (2 hours maximum) to provide the Flinders support teams an overview of the work that has been completed and ensure effective knowledge transfer.

The proposed engagement will be broken into several stages with a Go / No Go decision points after each stage. A summary of each stage is provided below.

**Stage 1 – Tool evaluation**

Flinders University are seeking a comprehensive review of the Microsoft 365 security and controls that form part of the E/A5 agreement in relation to data management and security (primarily via Purview). The review should include an evaluation of the Microsoft tooling and comparison with other third-party solutions, taking into consideration the following –

1. **Identification of data**
2. Labelling of data
3. Scope of data (Microsoft 365 data repositories but also capabilities to include other sources such as traditional on-premise network based storage)
4. Data life cycle management
5. Data security controls including data loss prevention, conditional access, data life cycle management, information protection etc.

As part of the evaluation, we are also wanting to answer the following question -

Q - Why should we consider another tool when we already have access to the Microsoft E/A5 license

**Stage 1 Go / No Go requirements**

The tool evaluation has been completed and

**Go** – we are confident the Microsoft E/A5 suite of tools meet our needs

OR

**No Go** – we are not confident the Microsoft E/A5 suite of tools meet our needs, and we should consider other third party tools

**Stage 2 – Manual Data Labelling pilot**

Flinders University are seeking to perform a small pilot of manual data labelling across the unstructured data repositories within the Microsoft 365 environment. The requirement of this stage is to complete the technical implementation of manual data labels within Microsoft Purview aligned with our established taxonomy and the deployment of any associated plug in or configuration requirements for end users to support the labelling of documents.

Flinders University will be responsible for :

All technical change management

Identification of, and all communication with pilot users

Development of user guides and associated training material

Stage 2 should also include technical handover and knowledge transfer for the Flinders Microsoft 365 support team to ensure ongoing operational support and future enhanced are possible.

**Stage 2 Go / No Go requirements**

The manual data labelling pilot has

**Go** – been successfully delivered and well received by the pilot users

**No Go** – not been successfully delivered and a review of next steps is needed

**Stage 3 – Considerations for next steps (Manual vs automatic labelling)**

Once manual labelling has been successfully piloted within university, we are seeking recommendations for next steps. This should include consideration for a broader, University wide rollout of the manual data labelling and consideration for automatic labelling and trainable classifiers.  Additionally, we would like to understand the process and effort required to extend the purview capabilities to additional unstructured data repositories such as on-premise traditional network storage and the steps to begin protecting data in line with Microsoft best practice (DLP, Conditional access etc)

Note that this stage is to support a future state and develop an appropriate deployment plan for the proposed next steps (including recommendations for managing pre-existing artefacts). This information would then be used to develop an internal design authority submission, the technical implementation of the future state would be undertaken as a separate Service Order released to panel members under 3.1 Microsoft 365