AZURE INFORMATION PROTECTION
DEPLOYMENT OPTIONS

Many organisations have implemented remote working and cloud data services like SharePoint, Teams and OneDrive and may now be at risk of data loss or misuse. Implementing an Information Protection strategy reduces the risks associated with the possession of large amounts of unstructured data in various repositories.

Insentra's methodology uses a combination of Azure Information Protection (AIP), Data Loss Prevention (DLP) - and optionally Torsion Information Governance and Microsoft Cloud App Security (MCAS) - to help identify and protect information across your entire estate.

Insentra offer two solutions for deployment of Information Protection, Light and Full.

LIGHT (M365 E3)

- Enablement of AIP
- Definition of your classification taxonomy
- Development of the Framework document
- Configuration of Data Loss Prevention (DLP)
- Integration into Conditional Access & Intune If deployed
- End-user enablement
- Optional - enable Torsion in your environment
- Setup governance of the solution for future success

Light Service will take approximately 3 weeks.

FULL (M365 E5), LIGHT SERVICE PLUS

- Expansion to other business scenarios
- Configuration of Microsoft Cloud App Security
- Shadow IT assessment (can be done In E3 If the right tools are in place)
- Automatic labelling (simulations across estate)
- Optional - expand Torsion deployment to protection

Full Service can take up to 8 weeks.

The deployment can also be supplemented with the following services:

- Torsion governance platform – answers the question "who has access to what, and why?", across SharePoint, Teams, on-premises file shares and more. Perfect for any situation where auditing is involved.
- Azure Information Protection Scanner – run scans against on-premises file shares to identify information in different areas
- Expand protection to other 3rd party products like GSuite and Box

The outcomes from the AIP Deployment are:

- Gain visibility of what information you possess, where its located and how it's being used, or shared
- Establish a framework for users to reference when classifying documents
- Start your journey to compliance frameworks like ISO 27001
- Begin your information protection strategy in the correct way