TECHNICAL AND FINANCIAL PROPOSAL FOR MICROSOFT PURVIEW DEPLOYMENT

VERSION 1.0

DATE: 06-08-2025 AD

Prepared by: Trusted Vision Company for CYBERSECURITY

Contact Information

Please feel free to contact the following individuals for information about this document:

Name	Hashem Al-Azizi
Mobile Phone	+966-53-122-1580
Email	Hashem.azizi@trustedvision.biz
Address	Cordoba District, Saeed Bin Zaid Street, Injaz Group Building, No. 6482, First Floor, P.O. Box: 13247, Riyadh, Kingdom of Saudi Arabia

Table of contents

1. Executive Summary

This proposal outlines the scope, objectives, and methodology for conducting a comprehensive technical assessment of the currently deployed Microsoft Purview solution. The aim is to validate its configuration, evaluate the effectiveness of data protection controls, identify areas of improvement, and provide actionable recommendations to enhance data governance, compliance, and operational efficiency. This engagement will ensure alignment with organizational security goals, national regulatory requirements (e.g., NCA), and global best practices.

2. Microsoft 365

Microsoft 365 is an integrated suite of cloud-based productivity, collaboration, and security tools designed to enable modern, secure, and efficient work environments. It combines well-known applications such as Word, Excel, PowerPoint, Outlook, Teams, SharePoint, and OneDrive, along with enterprise-grade services that support digital transformation, enhance communication, and streamline business operations.

The **Microsoft 365 E5** license is the most comprehensive offering within the Microsoft 365 family. It includes all features of the E3 license, with added capabilities in **advanced security, compliance, analytics, and voice solutions**. Specifically, the E5 license provides access to Microsoft Purview solutions for **data loss prevention (DLP)**, **sensitivity labeling**, **information protection**, **insider risk management**, **data lifecycle management**, and **compliance management** — making it a powerful choice for organizations with high regulatory and security requirements.

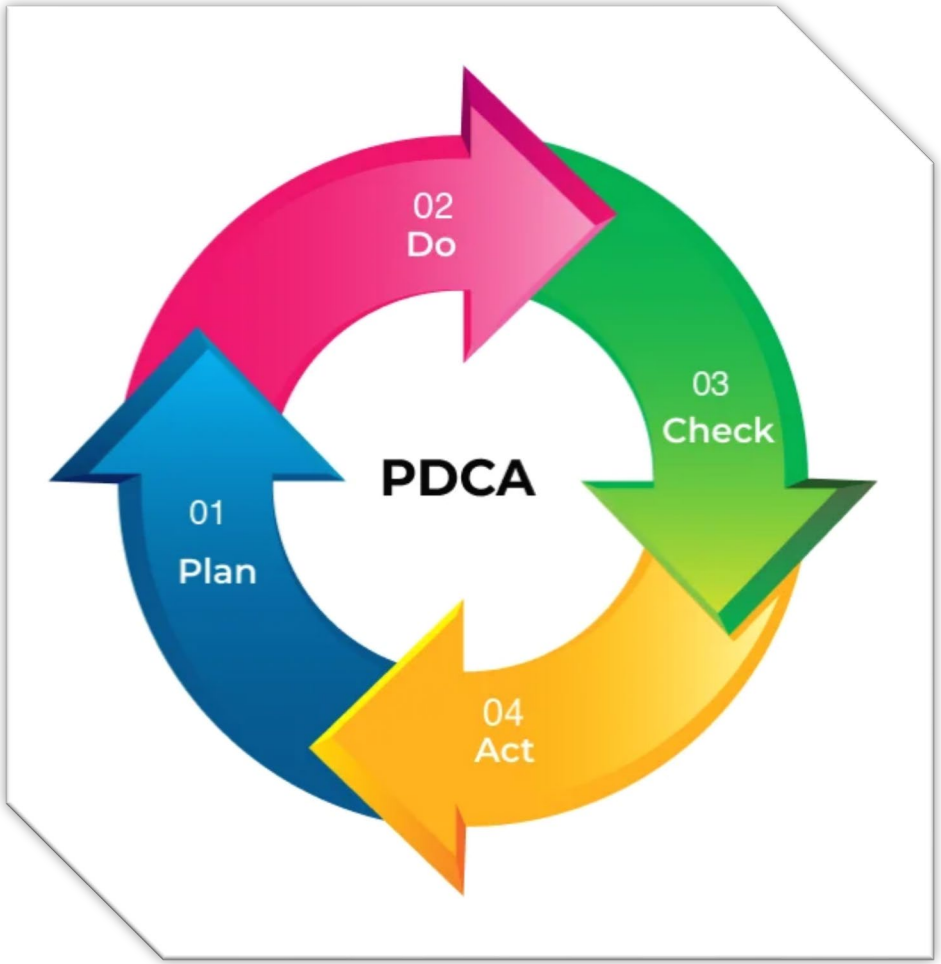
With E5, organizations benefit from:

- **Advanced threat protection** with Microsoft Defender
- **Cloud app security** and identity governance
- **Comprehensive compliance tools**, including data classification, auto-labeling, and audit
- **Unified endpoint management**
- **Enhanced analytics** with Power BI Pro

These capabilities make Microsoft 365 E5 a strategic solution for organizations aiming to strengthen their security posture, ensure compliance with frameworks like **NCA, GDPR, and ISO**, and maximize operational efficiency through intelligent tools and automation.

3. Project Methodology

In this project we will be following PDCA methodology, where we Plan for each phase or activity then Do execute the as the plan then, Check the outcome of the phase or activity and take actions based on the results.



PDCA methodology illustration:

No#	Phase	Activities must be conducted by Trusted Vision	Activities must be conducted by entity	Deliverables
1	Plan	• Understand customer requirements (such as in-use protection, portability, coverage, etc.). • Review the current environment (licenses, settings, policies). • Identify gaps and current risks. • Prepare a policy implementation plan (DLP, MIP, labeling, etc.).	• Provide the necessary access rights to the environment. • Share any internal/legislative documents or requirements.	• Current state analysis report. • Implementation Roadmap. • Capability and Coverage Assessment Report • Gap Register — including detailed observations and risk levels

2	Do	• Set up and implement DLP, MIP, and auto-labeling policies. • Enable Endpoint DLP and connect devices. • Configure integration with a SIEM such as Sentinel or a third-party solution. • Set up escalation and alerting mechanisms.	• Ensure policies are approved by the responsible authorities. • Support Agent installation on target devices.	• Microsoft Purview Environment by real-world policies • Policies are published and enabled on users/devices.
3	Check	• Review alert results and policy effectiveness. • Analyze false positives/false negatives. • Review coverage of applications and users.	• Providing user feedback (whenever false alerts or obstacles occur). • Facilitating testing and monitoring sessions.	• Policy performance report. • Recommendations for improvement (improving controls, adding exceptions, etc.).

				• Technical Evidence Pack — screenshots, logs, and configurations
4	Act	• Edit policies to improve accuracy and coverage. • Propose a mechanism for periodic review.	• Approval of amendments and improvements. • Allocating resources for sustainability monitoring.	• Improved and stable policies. • Policy Tuning Recommendations • Executive Summary Report — Key actions, key risks, decisions needed

4. Objectives

1. Assess the current-state implementation of Microsoft Purview.
2. Validate the effectiveness and coverage of existing policies and features.
3. Identify misconfigurations, operational gaps, and optimization opportunities.
4. Recommend improvements to extend capabilities and ensure full compliance with security and data protection requirements.

5. Scope Areas

- **Solution Review:**
  - Evaluate the configurations for DLP, data classification & labeling, and Information Rights Management (IRM).
  - Analyze current effectiveness and governance levels of the implemented solution.
  - Review the implementation of auto-labeling and content-based detection.
- **Configuration and Feature Review:**
  - Assess misconfigurations and tuning opportunities.
  - Review unused features and provide benefit/cost/risk analysis for deployment.
- **Coverage Areas:**
  - **Data in Transit:** Internal/external emails, web uploads, FTP/SFTP traffic.
  - **Data at Rest:** Discovery scans across shared drives and storage.
  - **Data in Use:** Controls on applications, clipboard, screenshots, USB, print jobs, etc.
- **Policy Analysis:**
  - Evaluate policy structures, templates, exceptions, and change control processes.
  - Recommend tuning to reduce false positives/negatives.
- **Technology Coverage:**
  - Microsoft Office and editors across platforms.
  - Collaboration platforms: Teams, Zoom, etc.
  - Archives, encrypted files, web inspection, endpoints (Windows/macOS/Linux), mobile, removable media, printing, clipboard.

- Cloud storage and SaaS services.
- File types: PDF, image scans, exports (bak, .sql, .csv).

- **Integration Review:**
  - Assess integration with SIEM for alerting.
  - Ensure availability of full audit trials for all administrative and end-user actions.
- **Licensing Evaluation:**
  - Review current licenses and coverage against features in use.
  - Advise on potential licensing upgrades for improved coverage.
- **Compliance Assessment:**
  - Validate alignment with NCA and internal compliance requirements.
- **Knowing Issues and Gaps**
  - PDF dynamic watermark not working on Windows after Microsoft Office update.
  - Auto-labeling based on keywords not functioning on Windows clients.
  - Sensitivity Labels limitations in on-prem mailboxes when accessed via mobile or OWA.

6. Technical Support Rols:

Data Loss Prevention (DLP):

1. Review and evaluate DLP policies applied in a Microsoft Purview environment.
2. Modify and develop DLP policies based on analysis results and technical recommendations.
3. Extract and analyze incident logs and reports related to policy implementation.
4. Evaluate policy coverage for data in three scenarios:
    - Data-in-Transit.
    - Data-at-Rest.
    - Data-in-Use.
5. Verify the accuracy of policy rules and reduce false positives by analyzing events and running policies in test mode.
6. Identify technical gaps in configuration or poor coverage for certain environments or applications.
7. Document the current configuration, modified policies, and their impact.

Data Classification and Labeling:

1. Review and document current Sensitivity Labels settings and labeling policies.
2. Verify the activation of Auto-Labeling policies and evaluate their effectiveness across platforms and systems.
3. Test and evaluate manual and automatic labeling experiences across various applications (Outlook, Office Apps, Teams) and operating systems (Windows).
4. Support coordination of technical troubleshooting procedures (such as Auto-Labeling failures) in collaboration with Microsoft Support.
5. Implement direct improvements to labeling policies based on usage analysis, such as:
6. Resetting Auto-Discovery conditions.
7. Modifying policy scopes to include or exclude specific groups.
8. Improve User Justification and Default Labels settings.
9. Provide technical and implementation recommendations to improve integration between labeling, DLP, and protection policies.

Information Rights Management (IRM):

1. Review Information Rights Management (IRM) settings and document the policies applied to documents and files.
2. Test the effectiveness of IRM restrictions (such as preventing copying, printing, and sharing content) on classified files.
3. Diagnose technical issues such as PDF Dynamic Watermark failure on Windows systems after updates.
4. Support the client team in following up on open support issues with Microsoft and providing the necessary technical data.
5. Verify the integration of IRM policies with classification and DLP to ensure comprehensive and accurate content protection.

7. Out of scope

1. Setting up or configuring any tools other than DLP, Classification/Labeling, or IRM.
2. Configure or adjust Active Directory, Intune, or infrastructure settings.
3. Tracking FTP/SMTP traffic is out of scope, as Microsoft Purview does not natively support monitoring or controlling FTP or SMTP protocols. Alternative third-party solutions or network-level proxies would be required to achieve such functionality.
4. Support for data protection features on Linux OS is limited to Microsoft Purview. Core functionalities such as Endpoint DLP and sensitivity labeling are not fully available or supported.
5. OCR-based detection (e.g., scanning image files or scanned PDFs for embedded text) is not natively supported by Microsoft Purview alone. To enable this functionality, integration with Azure Cognitive Services – OCR is required. Without this integration, image content will not be processed by DLP or auto-labeling engines.
6. Microsoft Purview does not support direct inspection of raw database files through DLP or auto-labeling.
7. Scanning of live databases is only possible if connected and configured as supported data sources (e.g., Azure SQL, SQL Server via scan rules).

8. Assumptions

1. **Access and Permissions**

   The client will provide all required administrative access and permissions to the Microsoft 365 compliance portal, Microsoft Purview, and endpoint devices as needed to review and configure DLP, data classification/labelling, and IRM.

2. **Licensing**

   The client has an active Microsoft 365 E5 license (or equivalent) with access to Microsoft Purview compliance features, including Data Loss Prevention (DLP), Information Protection (MIP), auto-labelling, and audit logs.

3. **Scope Limitation**

   This engagement includes **review and configuration only for** the following tools:

   - **Data Loss Prevention (DLP)**
   - **Data Classification & Sensitivity Labelling**
   - **Information Rights Management (IRM)**

   No other features (e.g., Insider Risk, Communication Compliance, Advanced eDiscovery) will be configured unless explicitly agreed upon.

4. **Client-Side Readiness**

   Client IT support will be responsible for:

   - Ensuring targeted endpoint devices are onboarded to Microsoft Defender for Endpoint (MDE).
   - Verifying that devices are Azure AD joined, or Hybrid Azure AD joined.
   - Supporting the deployment and validation of Endpoint DLP configurations, including:
   - Providing remote access or required administrative permissions.
   - Assisting with any Intune-related configurations (if applicable).
   - Verifying agent status and health on endpoint devices.
   - The engagement does **not** include development of custom scripts, connectors, or third-party integrations.

5. **Third-party Services**

Features that depend on **Azure AI**, **Azure Cognitive Services**, or **third-party OCR** (e.g., image scanning) are **not in scope** unless these services are already provisioned and integrated by the client.

6. **Change Control and Approvals**

   Any policy deployment or update will only be executed after written approval from the client or designated approvers.

7. **The expected duration for the project is 3 months, depending on the client's environmental readiness and the availability of required access. The timeline may be extended if delays occur due to client-side dependencies, lack of access, or technical blockers.**

9. User Acceptance Criteria

Tool	Use Case	Acceptance Criteria	Result	
			Pass	Fail
Data Loss Prevention (DLP)	Detect sharing of sensitive data via email	An alert is generated when sensitive info (e.g., ID, bank details) is sent externally	If alert is triggered	If not or incorrectly triggered
	Prevent upload of sensitive files to external websites	Upload is blocked or warning is shown when uploading sensitive file	If upload is blocked/warned	If unrestricted
	Controlled usage of USB ports	File transfer to USB is blocked or monitored as per policy	If blocked or tracked	If unrestricted
	Monitor print or copy operations of classified data	Print or copy actions for classified documents are logged or blocked	If logged or blocked	If not logged or unrestricted
Data Classification & Labeling	Automatically apply classification on document creation or email receipt	Proper label is automatically applied when sensitive data is detected	If auto-label applied	If missed or wrong label
	Enable user to manually choose classification label	Classification bar appears in Office apps and allows user to choose	If label bar visible and functional	If hidden or inactive

Information Rights Management (IRM)	Restrict forwarding, copying, or printing of classified documents	Restricted actions (forward, copy, print) are enforced on classified documents	If restrictions enforced	If actions still possible
	Expire document access after a specific period	Document becomes inaccessible after expiry time defined in policy	If document access expires	If still accessible

10. Team Specifications

Name	Title	Method
Abdullah Azizi	Cybersecurity Technical Analyst	On-Site
Seham Qahtani	Cybersecurity Technical Analyst	On-Site
Ghayda Harran	GRC Consultant	Remote