SOP: Data Loss Prevention (DLP) Policy Management

Owner: IT Security & Compliance Department
Version: 1.2
Date Created: 2025-06-15

Table of Contents

1. Purpose

This SOP defines the detailed workflow for configuring, enforcing, monitoring, and refining Data Loss Prevention (DLP) policies across the Microsoft 365 cloud and endpoint environments using Microsoft Purview. The goals are to protect sensitive data, enforce internal data handling policies, and uphold regulatory compliance standards.

2. Scope

Applies to IT security and compliance teams responsible for DLP across:

- **Cloud services**: Exchange Online, SharePoint Online, OneDrive for Business, Teams
- **Endpoints**: Windows and macOS via Endpoint DLP
- **Browsers/SaaS egress**: Microsoft Edge and third-party uploads

3. Prerequisites

- Microsoft 365 E5 license (or equivalent with DLP features enabled)
- Roles assigned: *Compliance Admin*, *Security Admin*, or *Global Admin*
- Devices enrolled in Defender for Endpoint
- Defined list of critical data categories
- Approved policy use cases and organizational risk criteria

4. Procedures

4.1 Accessing the DLP Interface

1. Log in to the Microsoft 365 portal at https://purview.microsoft.com
2. In the left-hand navigation, expand **Solutions** and open **Data Loss Prevention**.
3. You will be redirected to the DLP overview page.

4.2 Creating a Cloud-Based DLP Policy

4.2.1 Initiate Policy Creation

1. Within the DLP interface, select **Policies** → click **+ Create Policy**.
2. Choose a template suitable for your data type (e.g., "Privacy - Financial") or select **Custom policy**.

3. Name the policy using standard naming convention: DLP_[Scope]_[Purpose]_[YYYYMM]

4. Draft a policy description stating the objective, coverage, and approval owner.

4.2.2 Assign Locations

1. Select relevant enforcement points:
    - **Exchange Online** (email and attachments)
    - **SharePoint Online** (site content)
    - **OneDrive**
    - **Microsoft Teams** (chat and channel)
2. Optionally exclude certain groups or service accounts to minimize false positives.

4.2.3 Define Detection Conditions

1. Add **Sensitive info types** (e.g., U.S. Social Security Number, credit card).
2. Optionally configure:
    - **Custom sensitive info types** (regex-based detection)
    - **Document fingerprints** for known-sensitive files
    - **Trainable classifiers** for advanced classification

4.2.4 Configure Automated Actions

1. Under action settings, define behavior upon match:
    - **Block or restrict access**
    - **Encrypt content** (if supported)
    - **Show policy tip** with customized user message
    - **Notify** user, manager, and compliance admin via email
2. Set override behavior:
    - Allow override with justification
    - Require approval before sharing
3. Include notification templates and designate recipients (e.g., compliance@company.com)

4.2.5 Choose Policy Mode

1. Select one of:
    - **Test with notifications** (recommended for first 7–14 days)
    - **Test without notifications** (silent testing)
    - **Enforce** (active blocking mode)
2. Document the reason for chosen mode and expected date of transition to enforcement.

4.2.6 Finalize and Document

1. Click **Next**, review summary, then **Create**.
2. Add policy entry to DLP register with:
    - Policy name, ID, scope, effective date, creator, and mode
3. Notify stakeholders (IT, Legal, InfoSec) that policy is active.

4.3 Configuring Endpoint DLP

4.3.1 On-board Devices

1. In DLP UI, select **Device onboarding** tool.
2. Download the recommended package (.zip) for Windows/macOS.
3. Distribute via Intune or SCCM to target device groups.
4. Verify deployment success via endpoint management console.

4.3.2 Define Endpoint Policy

1. Back in DLP interface, click **+ Create Policy** → select **Device**.
2. Name policy using DLP_Device_[Scope]_[YYYYMM] format.
3. Choose targeting attributes (OS, device groups, or users).
4. Set conditions based on:
    - Sensitive info types
    - File paths or application usage
5. Define enforcement actions:

- **Block write to USB**
- **Restrict clipboard operations**
- **Prevent printing**
- **Block uploads to unauthorized apps/sites**

6. Enable notifications and configure audit settings.
7. Save and record policy metadata.

4.4 Locking Browser and SaaS Upload Traffic

1. In the DLP interface, under **Device policies**, find *Browser & app* section.
2. Enable **Microsoft Edge inline protection**.
3. Add rules for:
   - Trusted domains (e.g., approved SaaS platforms)
   - Blocked destinations (e.g., public AI platforms)
4. Save and record filter lists and enforcement mode.

4.5 Monitoring Incidents and Response

4.5.1 Incident Discovery

1. Navigate to **Alerts** tab under DLP.
2. Use filters to detect:
   - **Policy broken**, **Blocked event**, **Override used**
3. Drill into each incident:
   - Identify user, file, location, and timestamp
4. Download or export logs for forensic analysis.

4.5.2 Incident Response

1. For each incident:
   - Alert manager and affected user
   - Assess need to revoke external link or reset permissions
   - Escalate high-risk cases to InfoSec team

2. Update internal **DLP Incident Log** with:
    - Incident ID, user, rule triggered, actions taken, date, reviewer
3. Review policy performance monthly to identify policy gaps or adjustment needs.

4.6 Reporting and Policy Updates

1. Go to **Reports → DLP Dashboard**.
2. Run and export reports by:
    - Policy usage
    - Incidents by type/user/location
3. Review trends and identify areas for improvements.
4. Schedule periodic policy tuning:
    - Adjust confidence thresholds
    - Refine exclusion/inclusion lists
    - Introduce new sensitive info types
5. For each change:
    - Document change rationale, updated fields, and time frame
    - Retest in **Test mode** before re-enforcing

5. Conclusion

This SOP delivers an end-to-end framework for deploying and managing DLP controls using the latest Microsoft Purview interface. It enables granular data protection across services and devices, supports auditability, and ensures continuous optimization to mitigate data exposure risks while maintaining operational compliance.