SOP: Policy Enforcement and Compliance for Data Access and Sharing

Date Created: 2025-06-13
Version: 1.0
Owner: IFC - IT Security Team

1. Purpose

This SOP outlines procedures to configure, enforce, and monitor data access and sharing policies in SharePoint and OneDrive using the Microsoft 365 Admin Center and Microsoft Purview Compliance Center. It ensures that organizational data sharing remains secure, regulated, and auditable in compliance with standards such as GLBA, IRS 4557, and internal policies.

2. Scope

This SOP applies to all Microsoft 365 administrators responsible for securing data stored in and shared via:

- SharePoint Online
- OneDrive for Business
- Microsoft Purview

3. Prerequisites

- Admin access to the following:
    - Microsoft 365 Admin Center
    - SharePoint Admin Center
    - Microsoft Purview Compliance Center
- Predefined list of sensitive information types and compliance objectives
- Internal data classification policy
- Approved list of external domains (if restricting guest access)

4. Procedures

4.1 Configure Tenant-Level Sharing Settings (SharePoint/OneDrive)

1. Go to Microsoft 365 Admin Center → Admin centers → **SharePoint** → **Policies** → **Sharing**
2. Set the **SharePoint and OneDrive external sharing level** to **"Only people in your organization"**
3. Under **Link permission**, set default to **"View only"**

4. Save settings

4.2 Configure Site-Level Sharing Settings

1. Go to SharePoint Admin Center → **Sites** → **Active Sites**
2. Select the target site
3. Click **Settings**, then expand **External File Sharing** dropdown and control the access.
4. To Set a more restrictive level if needed, click on **More Sharing Settings** > **Advanced settings for external sharing.**
5. Configure:
    - **Guest access expiration**
    - **Default sharing link type**
6. Save changes

4.3 Create and Enforce DLP Policies (Microsoft Purview)

1. Go to Microsoft Purview Compliance Center > Solutions > **Data Loss Prevention** → **Policies**

2. Click **+ Create policy**
3. Choose a template (e.g., Financial, PII, Custom) or start from scratch
4. Name your policy (e.g., "SharePoint - PII DLP Policy")
5. Select **Locations** → Enable:
    - **SharePoint Online**

- **OneDrive for Business**

6. Define **Conditions**, e.g.:
   - Contains credit card number, SSNs, or custom keywords
7. Define **Actions** when matched:
   - Block sharing or access
   - Show policy tips
   - Send alerts to admins
8. Customize **User Notifications**:
   - Enable policy tips
   - Send emails to users and compliance officers
9. Select enforcement mode:
   - **Test with notifications** or **Turn on policy**
10. Click **Submit**, then document policy ID and scope

4.4 Monitor and Respond to DLP Incidents

1. Go to Microsoft Purview Compliance Center → **Reports → Data Loss Prevention**
2. Filter the report by: Policy name, Location (SharePoint or OneDrive), Severity or match count
3. Review each entry: What file was involved?, Who triggered the policy, Was the action blocked or allowed?
4. Take action: Notify user and manager, Revoke file access if necessary, Export logs for audit trail.
5. Document response in the Incident Register (include date, user, file, and remediation)

4.5 Configure Sensitivity Labels and Label Policies (Microsoft Purview Information Protection)

1. Microsoft Purview Compliance Center → **Information Protection → Labels**
2. Go to **Information Protection → Labels** → **+ Create a label**
3. Name the label (e.g., “Confidential – Internal Only”)

4. Define protection settings:
    - Encryption (restrict access to specific groups)
    - Content marking (headers/footers/watermarks)
5. Optionally, define auto-labeling conditions (e.g., contains SSNs)
6. Publish the label through a **Label Policy**:
    - Go to **Label policies** → **+ Publish labels**
    - Choose users/groups to apply it to
7. Confirm and save; document the label scope, policy name, and distribution

4.6 Configure and Enforce Domain Restrictions

1. Go to SharePoint Admin Center → **Policies → Sharing**
2. Scroll to **External sharing → More external sharing settings**
3. Enable **Allow only specific domains**
4. Enter a comma-separated list (e.g., partnercompany.com, govdomain.org)
5. Save and document the policy scope, rationale, and stakeholder approval

5. Conclusion

This SOP establishes a consistent, compliant framework for managing access and sharing of organizational data using Microsoft 365 tools. By enforcing tenant-wide and site-specific restrictions, and layering DLP monitoring on top, organizations can minimize risk exposure and meet security obligations. Regular monitoring ensures policies remain aligned with real-world user behavior and evolving regulatory requirements.