SOP: Reporting and Auditing – M365 Activity, Security, and Compliance Reports

Date Created: 2025-06-15
Version: 1.0
Owner: IFC-IT Security Team

Table of Contents

1. Purpose

This SOP provides guidelines to generate, review, and act upon reports related to user activity, security events, and regulatory compliance using Microsoft 365 tools. These reports support proactive risk management, enhance policy enforcement, and enable continuous improvement in security posture.

2. Scope

This SOP applies to all IT security, compliance, and administrative personnel responsible for auditing and reviewing activity across:

1. **Microsoft 365 Audit Logs** (user actions, file access, admin activity)
2. **Microsoft 365 Defender Reports** (security alerts, incidents, and risk detections)
3. **Microsoft Purview Compliance Reports** (DLP matches, sensitivity label usage)
4. **Entra ID Sign-in and Audit Logs** (user login events, access attempts)

3. Prerequisites

- Global Admin, Security Admin, or Compliance Officer permissions
- Enabled audit logging (Microsoft Purview)
- User activity and security data retention policies configured
- Microsoft 365 E3/E5 license (or equivalent access to Defender and Purview)

4. Procedures

4.1 Enable and Verify Audit Logging

Log in to the **Microsoft Purview Compliance Center**

1. Navigate to **Audit → Audit Search**
2. If not already enabled, click **Start recording user and admin activity**
3. Audit logs will begin collecting from this point forward (no retroactive data)
4. Confirm activation by searching for a recent user activity (e.g., file viewed)

4.2 Generate Microsoft 365 Audit Reports (User and Admin Activity)

Go to Microsoft Purview Compliance Center → **Audit → Audit Search**

1. Choose the **Activity Type** (e.g., “File accessed”, “Mailbox login”, “Deleted file”, “Sharing invitation sent”)
2. Define **Date Range** (up to 180 days for E5 licenses)
3. Specify **Users** or leave blank for org-wide search
4. Click **Search**
5. Export report to CSV or Excel for review
6. Document and escalate any suspicious activity as needed

4.3 Generate DLP and Sensitivity Label Reports

1. In **Purview**, go to **Reports → Data Loss Prevention**
2. Filter by:
    - Policy name (e.g., "SharePoint PII Block")
    - Action taken (e.g., “Blocked”, “Reported”)
3. Review:
    - Files and users that triggered rules
    - Frequency and severity of violations
4. Export and store for monthly compliance reviews

For **Sensitivity Label Usage**:

- Go to **Reports → Information Protection**
- Analyze label distribution trends, auto-labeling triggers, and overrides

4.4 Review Microsoft 365 Defender Reports (Security Events)

1. Go to **https://security.microsoft.com**
2. Navigate to **Reports → Threat Protection Status**
3. View trends in:
    - Email threats (malware, phishing)

    - Compromised accounts
    - Device vulnerabilities
4. Under **Incidents & Alerts**, filter unresolved incidents
5. Drill down into high-severity events
6. Take follow-up actions: isolate devices, reset credentials, block users

4.5 Review Entra ID Sign-In and Audit Logs

1. Go to **https://entra.microsoft.com**
2. Navigate to **Monitoring → Sign-in logs**
    - Review user login activity, device location, app access
    - Filter for failed or risky sign-ins
3. Go to **Audit Logs** to review:
    - Role assignments
    - Policy changes
    - User modifications
4. Export logs and attach to audit trail documentation
5. Escalate unusual patterns (e.g., repeated login failures from unknown IPs)

5. Conclusion

Effective reporting and auditing are foundational to securing Microsoft 365 environments and ensuring compliance. This SOP outlines a structured, consistent approach to monitoring user behavior, detecting anomalies, and responding to policy violations. Regular use of these reports helps mitigate risks, strengthens accountability, and drives continuous security improvement.