

SOP-M365-001__Governance__v1.0.0

SOP-M365-001__Governance__v1.0.0

Standard Operating Procedure: Microsoft 365 Governance and Administration

Document ID	SOP-M365-001
Version	1.0
Effective Date	2025-12-02
Author	M365 System Administrator
Approver	Director, IT Operations

1.0 Purpose

This Standard Operating Procedure (SOP) establishes the policies and operational procedures for the governance and administration of the Microsoft 365 ecosystem. The primary objective is to ensure compliance, data security, operational continuity, and standardized management across all M365 services.

2.0 Scope

This SOP applies to all Microsoft 365 services, including but not limited to:
- Identity and Access Management (Microsoft Entra ID) - Data Governance (SharePoint Online, Exchange Online, OneDrive) - Information Governance (Microsoft Purview) - Device Governance (Microsoft Intune) - Automation and Application Governance (Power Platform) - Hybrid Cloud Configurations

This document is intended for M365 Administrators, Security & Compliance Officers, and IT support personnel responsible for managing the M365 environment.

3.0 Core Governance Domains & Procedures

This section outlines the standard procedures for key governance tasks, categorized by domain.

3.1 Identity & Access Governance (Entra ID)

Objective: Manage user identities, control access to resources, and enforce security policies.

Task	Procedure / Portal Path	PowerShell Cmdlet
Connect to M365	N/A	<code>Connect-MgGraph -Scopes "RoleManagement.Read.All"</code>
Review Admin Roles	Entra ID > Roles & Admins > Roles	<code>Get-MgRoleDefinition</code>
Enable MFA	Entra ID > Protection > Multi-Factor Authentication	Use Conditional Access Policies
Conduct Access Reviews	Entra ID > Identity Governance > Access Reviews	<code>New-MgIdentityGovernanceAccessReviewScheduleDefinition</code>
Assign PIM Role	Entra ID > Privileged Identity Management > Assign eligibility	<code>New-MgRoleManagementDirectoryRoleEligibilityScheduleDefinition</code>

3.2 Data & Information Governance (Purview, SharePoint, Exchange)

Objective: Manage the data lifecycle, apply protection policies, and ensure compliance with retention requirements.

Task	Procedure / Portal Path	PowerShell Cmdlet
Create Retention Policy	Microsoft Purview > Data Lifecycle Management > Retention Policies	<code>New-RetentionCompliancePolicy</code>
Apply Sensitivity Label	Microsoft Purview > Information Protection > Labels	<code>Set-Label</code>
Enable Audit Logging	Microsoft Purview > Audit > Start Recording user and admin activity	<code>Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true</code>

Task	Procedure / Portal Path	PowerShell Cmdlet
Create eDiscovery Case	Microsoft Purview > eDiscovery (Standard or Premium) > Create a case	New-ComplianceSearch
Create Mail Retention Tag	Exchange Admin Center > Compliance Management > Retention Tags	New-RetentionPolicyTag

3.3 Device Governance (Intune)

Objective: Enforce security and compliance policies on all corporate and personal devices accessing M365 resources.

Task	Procedure / Portal Path
Create Compliance Policy	Intune Admin Center > Devices > Compliance Policies > Create Policy
Enroll Devices (Autopilot)	Intune Admin Center > Devices > Enrollment > Windows Autopilot Deployment Program
Deploy Disk Encryption	Intune Admin Center > Endpoint Security > Disk Encryption > Create Policy
Assign App Protection	Intune Admin Center > Apps > App Protection Policies > Create Policy

3.4 Automation Governance (Power Platform)

Objective: Control and monitor the use of Power Automate and Power Apps to prevent data leakage and ensure operational stability.

Task	Procedure / Portal Path
Enforce DLP Policy	Power Platform Admin Center > Policies > Data Policies > New Policy
Review Flow Ownership	Power Automate > Solutions > Select Solution > Review Owners
Audit Flow Activity	Power Platform Admin Center > Analytics > Power Automate > View (Runs, Usage, Created)

3.5 Hybrid & Integration Governance

Objective: Manage the secure integration between on-premises infrastructure and Microsoft 365 cloud services.

Tool / Technology	Procedure
Hybrid Identity Sync	Use Azure AD Connect to synchronize on-premises Active Directory with Entra ID. Monitor sync status via the AAD Connect Health portal.
Hybrid Mail Flow	Run the Exchange Hybrid Configuration Wizard (HCW) to establish and verify mail flow. Regularly review transport rules and connectors.
SharePoint Hybrid	Use the SharePoint Hybrid Configuration Wizard in SharePoint Central Administration to configure hybrid search, profiles, and taxonomy.

4.0 Roles and Responsibilities

- **M365 Administrator:** Responsible for the overall configuration, maintenance, and day-to-day administration of the M365 tenant as outlined in this SOP.
- **Identity & Access Administrator:** Specializes in managing Entra ID, PIM, Conditional Access, and identity lifecycle.
- **Information Protection Administrator:** Manages data classification, retention policies, sensitivity labels, and DLP within Microsoft Purview.
- **Endpoint Administrator:** Manages device compliance, enrollment, and application protection policies via Microsoft Intune.

5.0 Appendix

5.1 Training and Certification Path

Personnel are encouraged to pursue the following certifications to ensure proficiency in M365 governance:

Tier	Certification	Focus Area
Foundational	MS-102: Microsoft 365 Administrator	Centralized administration, identity, security, and compliance.
Foundational	SC-900: Security, Compliance, and Identity Fundamentals	Core concepts of Microsoft's security and compliance suite.
Associate	SC-300: Identity & Access Administrator	Entra ID, PIM, Conditional Access, Access Reviews.
Associate	MD-102: Endpoint Administrator	Intune, Autopilot, Device Compliance, Application Management.
Associate	MS-740: Troubleshooting Microsoft Teams	SharePoint Admin Center, retention, hybrid setup
Expert	SC-100: Cybersecurity Architect Expert	Enterprise-wide security framework design and implementation.

5.2 Key Resources

- **Microsoft Learn (Official Training):**
 - M365 Administrator Path
 - SC-300 Identity & Access Path
 - MD-102 Endpoint Administrator Path
- **Hands-on Labs:**
 - **M365 Developer Sandbox:** developer.microsoft.com/en-us/microsoft-365/dev-program
 - **Official Microsoft Labs:** microsoftlearning.github.io/Labs/