Enterprise Identity & Access Governance Policy

Using Microsoft Entra ID

Document Title: IAM Governance Policy

Version: 1.0

Author: Leul Nigussie

Organization: [Insert Your Lab/Project/Portfolio Name]

Date of Issue: [Insert Date]

# 1. Purpose

This policy defines the structure and controls for managing identities, access, and privileged roles using Microsoft Entra ID. It supports secure identity lifecycle management (Joiner-Mover-Leaver), conditional access enforcement, access reviews, and role governance through Microsoft Entra ID Governance and Privileged Identity Management (PIM).

# 2. Objectives

• Ensure secure, least-privilege access to enterprise systems.

• Prevent unauthorized access via conditional access and PIM.

• Comply with NIST SP 800-53, ISO 27001, and zero trust principles.

• Automate identity lifecycle (JML) to reduce human error and delays.

• Periodically audit and review high-privilege accounts and guest users.

# 3. Scope

This policy applies to:

• All internal users with access to Microsoft 365 or Azure resources.

• External users invited as guests into Microsoft Entra ID.

• Admins and users assigned elevated roles through PIM.

• Applications integrated with Entra ID for SSO and RBAC.

# 4. Identity Governance Components

This section includes four main components:

1. Conditional Access Policies

2. Privileged Identity Management (PIM)

3. Access Reviews

4. Joiner-Mover-Leaver (JML) Automation

# 4.1 Conditional Access Policy Framework

• Block Legacy Authentication: Prevents use of insecure protocols (IMAP, POP).

• MFA Enforcement: Requires multi-factor authentication for all users, especially admins.

• Location-Based Restrictions: Limits access by IP or country to protect sensitive roles.

• Guest Access Controls: Limits access for external users to Teams, SharePoint only.

# 4.2 Privileged Identity Management (PIM)

• Assign high-risk roles (Global Admin, Security Admin) as 'eligible' with approval workflow.

• Role activations require just-in-time access with expiration and justification.

• Enable alerts for all PIM role activations and unusual access behavior.

• Quarterly reviews are conducted and inactive eligible roles are removed automatically.

• One break-glass admin account is excluded from PIM and stored securely offline.

# 4.3 Access Reviews

• Guest Access Reviews: Monthly auto-review of all guest accounts.

• PIM Role Reviews: Every 30 days for all sensitive roles.

• Group Membership Reviews: Bi-monthly review of dynamic and security group access.

• Use Entra ID automation to remove users with no justification or inactivity after 14 days.

# 4.4 Joiner-Mover-Leaver (JML) Automation

• Joiner: New hires added to dynamic groups and assigned access automatically.

• Mover: Role changes update group membership and access packages based on metadata.

• Leaver: Terminated users are immediately disabled, licenses revoked, access removed.

• Powered by Lifecycle Workflows in Microsoft Entra and Power Automate where applicable.

# 5. Monitoring, Audit, and Alerts

• Use Microsoft Entra audit and sign-in logs to monitor conditional access and role use.

• Alerts configured for risky sign-ins, PIM activations, failed MFA, and legacy auth.

• Weekly admin summary reports and daily incident alerts for IAM team visibility.

• Optional: Integrate with Microsoft Sentinel or Defender for Cloud Apps.

# 6. Policy Governance and Review

• Policy is reviewed every 6 months or after major platform/tenant changes.

• IAM Governance Committee must approve changes to this policy.

• Tracks change log and maps to compliance standards (NIST, ISO, CIS).

# 7. Document Change Log

Version: 1.0

Date: [Insert Date]

Author: Leul Nigussie

Summary: Initial version of the IAM Governance Policy for Microsoft Entra ID

# 8. References

• Microsoft Entra ID Governance Documentation

• NIST SP 800-53 Rev. 5 – AC and IA Controls

• ISO/IEC 27001:2022 – Access Control Clauses

• CIS Controls v8 – Controls 5 (Account Management), 6 (Access Control), 16 (Application Security)