IAM Governance Policy

1. Purpose

This IAM Governance Policy defines how the organization manages digital identities and controls access to its information systems. The goal is to enforce the principle of least privilege, reduce access-related risks, and align with NIST and Microsoft security best practices.

2. Scope

This policy applies to all users (employees, contractors, vendors, and guests) and covers all systems, applications, and services managed by the organization, whether on-premises or in the cloud (including Microsoft Entra ID, formerly Azure AD).

3. User Classifications

- Standard Users: Internal employees with role-based access to standard applications.
- Privileged Users: IT admins, developers, and security staff with elevated permissions.
- Vendors: Third parties with limited, time-bound access.
- Guests: External users collaborating on business projects via Microsoft B2B.

4. Identity Lifecycle Management

- Joiner: New hires are provisioned automatically based on HR integration, assigned to required groups and licensed.
- Mover: Internal transfers or promotions trigger access updates via dynamic group rules and manual review.
- Leaver: Accounts are disabled immediately upon offboarding, followed by access revocation and eventual deletion after 30 days.

5. Access Control and Role-Based Access

Access is granted based on least privilege principles through pre-defined roles. Each business unit uses RBAC to ensure users only access data necessary for their responsibilities. Access permissions are reviewed quarterly or upon role changes.

6. Authentication Requirements

- Multi-factor authentication (MFA) is mandatory for all user accounts.
- Privileged roles must re-authenticate with MFA during role activation or elevation.
- Legacy authentication protocols are disabled to prevent insecure access.
- Password policy includes complexity requirements, 90-day expiration, and lockout thresholds.

7. Privileged Identity Management (PIM)

- All elevated access (Global Admin, Security Admin, etc.) must be assigned as 'Eligible' through PIM.
- Activation requires: justification, MFA, approval (for selected roles), and a limited time window (e.g., 4

hours).

- PIM logs all role activations, which are forwarded to the SIEM for monitoring.

8. Guest Access Governance

- Guests are invited through a designated approval workflow and assigned limited roles.
- External collaboration settings restrict guest permissions to least privilege.
- Guest accounts automatically expire after 30 days unless renewed.
- Monthly guest access reviews are required by the resource owner.

9. Access Reviews

- Conducted quarterly for the following:
  - Privileged users
  - Guest users
  - Sensitive application access
- Access Review configurations are managed through Microsoft Entra ID and results are exported for audit purposes.
- Inactive or unverified accounts are automatically removed.

10. Monitoring and Logging

- All sign-in activities, role activations, and conditional access decisions are logged.
- Logs are retained for a minimum of 90 days and forwarded to the SIEM for analysis.
- Alerts are generated for high-risk sign-ins, excessive MFA failures, and unauthorized access attempts.

11. Enforcement

Violations of this policy may result in access revocation, disciplinary actions, or termination. The IAM Team and Security Operations Center are jointly responsible for enforcing this policy.

Document Owner: IAM Governance Team

Review Frequency: Annually

Next Review Date: June 2026