Azure Access Control Policy

Policy Number: IT-AC-001
Date Adopted: September 17, 2025
Last Revision: September 17, 2025
Last Review: September 17, 2025

1. Purpose

To define standards for granting, managing, and reviewing access to Entra ID and associated Azure resources, ensuring the principle of least privilege and secure identity management.

2. Applicability

This policy applies to:

- All employees, contractors, and third-party users accessing the organization's Entra ID and Azure environment.
- All Azure resources, including subscriptions, virtual machines, storage accounts, applications, and services.

3. Accountability

- **Employees and Contractors:** Must follow access assignment procedures and report any inappropriate access.
- **IT / Security Team:** Responsible for implementing, monitoring, and reviewing access controls.
- **Managers:** Ensure team members have only necessary access based on job responsibilities.

4. Definitions

- **Entra ID (formerly Azure Active Directory):** Microsoft cloud-based identity and access management platform.
- **Least Privilege:** Principle of granting users only the permissions necessary for their role.
- **Privileged Role:** Any role with elevated permissions (e.g., Global Admin, Subscription Owner).
- **Managed Identity / Service Principal:** Azure identity used for applications or automation scripts instead of shared credentials.
- **MFA (Multi-Factor Authentication):** Authentication method requiring more than one verification factor.

5. Policy

- All users must be assigned Entra ID roles based on job function and the principle of least privilege.
- Privileged roles require documented justification, managerial approval, and enforced MFA via Security Defaults or conditional access.
- Temporary elevated access must be granted via Azure Privileged Identity Management (PIM) and revoked automatically.
- Access reviews must be conducted quarterly to ensure that users have only the permissions required for their current roles.

6. Non-Compliance and Sanctions

Violations of this policy may result in:

- Revocation or modification of access privileges.
- Written warnings or other disciplinary action.
- Escalation to HR or management.
- Reporting to legal or regulatory authorities if required.