Azure Password & Authentication Policy

Policy Number: IT-PW-003
Date Adopted: September 17, 2025
Last Revision: September 17, 2025
Last Review: September 17, 2025

1. Purpose
To establish minimum password and authentication requirements for securing access to Entra ID and Azure resources.

2. Applicability
This policy applies to:

- All employees, contractors, and third-party users with access to Entra ID or Azure resources.
- All authentication mechanisms used to access Entra ID and Azure resources.

3. Accountability

- **Users:** Must comply with password requirements and use MFA.
- **IT / Security Team:** Responsible for enforcing authentication policies and monitoring compliance.
- **Managers:** Ensure team members follow password and MFA requirements.

4. Definitions

- **Multi-Factor Authentication (MFA):** Authentication method requiring two or more verification factors.
- **Self-Service Password Reset (SSPR):** Azure feature allowing users to securely reset passwords without IT intervention.
- **Password Complexity:** Requirement for uppercase, lowercase, numeric, and special characters.

5. Policy

- Passwords must be at least 12 characters and include uppercase, lowercase, numbers, and symbols.
- Passwords must be changed every 90 days, with the last 5 passwords blocked from reuse.
- MFA is required for all users, with special emphasis on privileged roles.
- Accounts are locked after 5 failed login attempts within 15 minutes, with auto-unlock after 30 minutes.

- Self-service password reset must be enabled with MFA verification.

6. Non-Compliance and Sanctions

Violations may result in:

- Account suspension or enforced password reset by IT
- Written warnings or other disciplinary action.
- Escalation to management or HR.
- Reporting to legal or regulatory authorities if required.