Password / Credentials Policy

MMF Consulting Grp (Pte. Ltd.)

September 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.2, CC6.7

Table 2: Document history

Date	Comment
Sep 18 2024	Initial document
Dec 3 2024	Updated MFA and lockout policies

1 Password / Credentials Policy

Field	Value
ID	PASSP-002
Effective Date	September 18, 2024
Last Revised	December 3, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Password Management Policy establishes requirements for creating, protecting, and managing passwords to ensure the security of MMF Consulting Grp (Pte. Ltd.) information systems. This policy applies to all employees, contractors, and third parties who access MMF Consulting Grp (Pte. Ltd.)'s systems and data.

1.2 Background

Strong password management is a critical component of MMF Consulting Grp (Pte. Ltd.)'s security strategy. As we handle sensitive client data including contracts and financial information, proper password controls work in conjunction with multi-factor authentication to provide robust access security. This policy leverages Microsoft Entra's capabilities while establishing clear standards for password creation and management.

1.3 Policy

1.3.1 Password Requirements

All passwords for MMF Consulting Grp (Pte. Ltd.) systems must meet the following minimum requirements:

1. **Length**: Minimum 12 characters
2. **Complexity**: Must contain at least three of the following:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters (!@#$%^&*)
3. **Uniqueness**: Cannot be the same as the previous 12 passwords
4. **Prohibited Elements**:
    - No dictionary words
    - No personal information (names, birthdays, addresses)
    - No company-related terms (MMF, audit, comply)
    - No keyboard patterns (qwerty, 123456)

1.3.2 Password Management Standards

1. **Multi-Factor Authentication (MFA) Requirements**
    - **Mandatory for All Systems**: Microsoft 365, Box.com, and any client systems
    - **Approved MFA Methods**:
        - Microsoft Authenticator app (preferred)
        - SMS to registered mobile device (backup)

    - Hardware tokens (for high-privilege accounts)
  - **MFA Device Management**:
    - Register personal mobile devices through Microsoft Entra
    - Report lost/stolen devices immediately to System Administrator
    - Maximum 2 registered devices per user
2. **Account Security and Management**
  - **Account Lockout**: Accounts automatically lock after 5 failed login attempts with 30-minute lockout duration
  - **Password Reset**: Must be performed through official Microsoft Entra self-service portal
  - **Password Storage**: Never write down or store in plain text; use approved password managers only
  - **Password Sharing**: Strictly prohibited; each user must have unique credentials
  - **Privileged Accounts**: Separate accounts required for administrative functions
  - **Service Accounts**: Managed by System Administrator with approval required
  - **Password Rotation**: Passwords do not expire due to MFA but must be changed if compromise is suspected

1.4 Policy Review and Maintenance

This policy is subject to annual review and update:

- **Annual Review**: Conducted each October by the System Administrator
- **Review Scope**: Policy effectiveness, industry standards, and compliance requirements

1.5 Exceptions

All exceptions to this policy require written approval from the Director, accompanied by documented business justification and formal risk assessment. Exception requests must demonstrate that alternative controls provide equivalent security protection or that the business risk is acceptable given operational requirements. Approved exceptions must include compensating controls and regular review schedules to ensure continued appropriateness.

1.6 Violations & Enforcement

Violations of this policy are subject to disciplinary action commensurate with the severity of the breach and its potential impact on organizational security. Enforcement measures may include immediate password reset requirements, mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Password sharing or credential compromise may result in immediate termination and potential legal action.

2 Authorship and Approval

Last edit made by Bill Li (yushengli.tw@gmail.com) on Mon, 18 Aug 2025 18:37:06 +0800.

Approved by Yusheng Li (YushengLi@users.noreply.github.com) on Thu, 21 Aug 2025 11:54:21 +0800 in commit 8e0c1296a6a80185ef11d1631bbf6ca59ccc896b.