Identity and Access Management Framework

MMF Consulting Grp (Pte. Ltd.)

September 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.2, CC6.3, CC6.4, CC6.7, CC6.8

Table 2: Document history

Date	Comment
Sep 25 2024	Initial document
Nov 15 2024	Enhanced RBAC and data controls

1 Identity and Access Management Framework

Field	Value
ID	ACP-002
Effective Date	September 25, 2024
Last Revised	November 15, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Access Control Policy establishes the framework for managing user access to MMF Consulting Grp (Pte. Ltd.) information systems and data. The policy ensures that access rights are granted based on documented business need, properly authorized, and regularly reviewed. This policy applies to all employees, contractors, and third parties requiring access to MMF Consulting Grp (Pte. Ltd.) resources.

1.2 Background

As a compliance auditing firm handling sensitive client data, MMF Consulting Grp (Pte. Ltd.) must ensure that access to information systems is strictly controlled and monitored. This policy implements the principle of least privilege, ensuring users have only the minimum access necessary to perform their job functions.

1.3 Policy

1.3.1 Access Control Principles

1. **Least Privilege**: Users receive only the minimum access required for their role
2. **Separation of Duties**: Critical functions are divided among multiple individuals
3. **Need-to-Know**: Access to confidential data requires documented business justification
4. **Defense in Depth**: Multiple layers of access control protect sensitive resources
5. **Accountability**: All access is attributable to individual users

1.3.2 Logical Access Control

1.3.2.1 User Account Management

- **Centralized Identity Management**: Microsoft Entra ID serves as the single source of identity for all users
- **Unique User Accounts**: Each individual is assigned a unique user account tied to their identity
- **Account Provisioning**: New accounts are created only upon formal authorization from HR and management
- **Role-Based Access Control (RBAC)**: Access permissions are assigned based on job functions and responsibilities
- **Account Deprovisioning**: Immediate account deactivation upon employment termination or role change

1.3.2.2 Multi-Factor Authentication (MFA) All user accounts must implement multi-factor authentication. Detailed MFA requirements, approved methods, and device management procedures are specified in the Password Management Policy (PASSP).

1.3.2.3 Access Levels and Permissions

- **Standard User Access**: Basic productivity applications and assigned client data
- **Senior Staff Access**: Additional client engagements and analysis tools
- **Administrative Access**: System management functions and user provisioning
- **Emergency Access**: Temporary elevated privileges for business continuity
- **Client-Specific Access**: Segregated permissions for different client engagements

1.3.2.4 Password and Credential Management

- **Password Complexity**: Minimum 12 characters with complexity requirements
- **Account Lockout**: Automatic lockout after 5 failed authentication attempts
- **Credential Sharing Prohibition**: Sharing of passwords or authentication devices strictly forbidden
- **Service Account Management**: Dedicated accounts for system services with complex passwords
- **Emergency Access Procedures**: Secure break-glass procedures for critical system access

1.3.2.5 Client Data Segregation

- **Engagement-Based Access**: Separate access controls for each client engagement
- **Data Compartmentalization**: Users can only access data for their assigned client projects
- **Cross-Client Restrictions**: Strict prevention of data mixing between different clients
- **Project Completion Access**: Removal of access upon engagement completion
- **Audit Trail Maintenance**: Detailed logging of all client data access activities

1.3.2.6 Quarterly Access Reviews

- **Comprehensive Review Process**: Systematic verification of all user access permissions
- **Manager Certification**: Direct supervisors certify appropriateness of subordinate access
- **Automated Reporting**: Microsoft Entra ID reports highlighting access changes and anomalies
- **Exception Documentation**: Formal documentation of any access exceptions or deviations
- **Remediation Tracking**: Prompt correction of inappropriate or excessive access permissions

1.3.3 Physical Access Control

1.3.3.1 Office Facility Security

- **Keycard Access System**: All office locations (Singapore, Taipei, and Hsinchu) require keycard authentication
- **Employee Access Cards**: Unique access cards are issued to all employees with role-based permissions
- **Visitor Management**: All visitors must sign in with HR/Legal Representative and receive temporary access badges only
- **Access Logging**: Electronic logs are maintained for all keycard access events and visitor entries
- **Lost Card Procedures**: Immediate deactivation and replacement process for lost or stolen access cards

1.3.3.2 Perimeter Security Controls

- **Security Cameras**: Monitoring systems installed at all office entrances, exits, and common areas
- **Reception Areas**: Controlled access points with receptionist or automated visitor management
- **After-Hours Access**: Special procedures and additional logging for evening and weekend access
- **Tailgating Prevention**: Policies requiring individual authentication and prohibiting following others through secured doors
- **Emergency Exits**: Secured emergency exits with alarm systems and access logging

1.3.3.3 Workspace Security

- **Clean Desk Policy**: Mandatory secure storage of confidential documents when workstations are unattended
- **Hot Desking Environment**: Flexible workspace assignment with secure storage lockers for personal items
- **Printer/Copier Security**: Controlled access to printing facilities with user authentication requirements
- **Confidential Meeting Rooms**: Enhanced access controls for rooms used for sensitive client discussions
- **Storage Areas**: Locked storage for sensitive documents, backup media, and equipment

1.3.3.4 Visitor Access Management

- **Pre-Authorization**: Advance notification and approval required for all non-employee visitors
- **Escort Requirements**: Visitors must be accompanied by authorized employees at all times
- **Visitor Badges**: Temporary identification badges with expiration times and area restrictions
- **Client Representatives**: Special procedures for client personnel requiring temporary access during audits
- **Vendor Access**: Controlled access for maintenance, delivery, and service personnel

1.3.3.5 Physical Asset Protection

- **Equipment Security**: Company laptops and devices secured with cable locks when left unattended
- **Secure Storage**: Locked cabinets and storage areas for spare equipment and sensitive materials
- **Asset Tracking**: Physical inventory tags and regular verification of equipment locations
- **Removal Authorization**: Formal approval process for removing company equipment from premises
- **Personal Property**: Clear separation between company and personal items in shared workspaces

1.3.3.6 Access Reviews and Compliance

- **Quarterly Physical Access Audits**: Regular review of physical access permissions and actual usage patterns
- **Access Recertification**: Annual verification that access levels remain appropriate for job functions
- **Terminated Employee Procedures**: Immediate revocation of physical access upon employment termination
- **Role Change Management**: Prompt adjustment of access permissions when job responsibilities change
- **Compliance Monitoring**: Regular testing of physical security controls and access management procedures

1.3.3.7 Multi-Location Coordination

- **Inter-Office Access**: Standardized procedures for employees visiting other office locations
- **Temporary Assignments**: Access management for employees temporarily working at different offices
- **Cross-Location Meetings**: Secure access procedures for multi-office meetings and collaborations
- **Emergency Contacts**: Local emergency contacts and procedures at each office location
- **Consistent Standards**: Uniform physical security standards applied across all office locations

1.3.4 Remote Access and Client Site Security

1.3.4.1 VPN Access Requirements

- **Mandatory VPN**: Required for all connections from unsecured networks (hotels, coffee shops, public WiFi)
- **Client Network Access**: Secure connection procedures when working at client facilities
- **Split Tunneling Restrictions**: All business traffic must route through company VPN
- **Connection Monitoring**: Logging and monitoring of all VPN connections and activities

- **Approved VPN Software**: Only company-approved VPN clients and configurations permitted

1.3.4.2 Client Site Access Procedures

- **Client Security Compliance**: Adherence to client-specific security policies and access requirements
- **Temporary Access Badges**: Coordination with client security for visitor access badges
- **Equipment Registration**: Registration of company devices with client IT security systems when required
- **Network Isolation**: Use of client guest networks or isolated network segments
- **Confidentiality Maintenance**: Protection of MMF and other client information while on-site

1.3.5 Access Control Monitoring and Enforcement

1.3.5.1 Continuous Monitoring

- **Real-Time Alerts**: Automated notifications for unusual access patterns or policy violations
- **Failed Login Monitoring**: Tracking and investigation of repeated authentication failures
- **Privileged Access Monitoring**: Enhanced monitoring of administrative and high-privilege account activities
- **Geographic Access Controls**: Alerts for access from unexpected geographic locations
- **Time-Based Restrictions**: Enforcement of business hours access policies where appropriate

1.3.5.2 Violation Response

- **Immediate Investigation**: Prompt investigation of all access control violations and anomalies
- **Account Suspension**: Temporary suspension of accounts involved in security incidents
- **Incident Documentation**: Detailed records of violations, investigations, and remediation actions
- **Progressive Discipline**: Escalating consequences for repeated or severe access violations
- **Legal Action**: Coordination with legal counsel for serious breaches or criminal activity

1.4 Policy Review and Maintenance

This policy is subject to annual review and update:

- **Annual Review**: Conducted each November by the Director and System Administrator
- **Review Scope**: Access control effectiveness, role definitions, and client data segregation
- **Audit Integration**: Quarterly access reviews inform annual policy updates
- **Compliance Verification**: Alignment with TSC criteria and client security 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 immediate investigation and disciplinary action commensurate with the severity of the breach and its potential impact on organizational security. Enforcement measures may include immediate access suspension, mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Unauthorized access attempts or privilege abuse may result in immediate termination.

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.