Mobile Device Policy

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1

Table 2: Document history

Date	Comment
Oct 15 2024	Initial document
Nov 30 2024	Policy updates and improvements

1 Mobile Device Policy

Field	Value
ID	MOBP-002
Effective Date	October 15, 2024
Last Revised	November 30, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Mobile Device Policy establishes security requirements and usage guidelines for mobile devices accessing MMF Consulting Grp (Pte. Ltd.) systems and data. This policy applies to all employees using personal mobile devices for business purposes and covers the limited business use of personal phones and tablets.

1.2 Background

MMF Consulting Grp (Pte. Ltd.) employees frequently travel to client sites and require mobile access to business communications. While company-issued laptops remain the primary work devices, controlled access to business email and communications via personal mobile devices enhances productivity while maintaining security. This policy balances operational needs with client data protection requirements.

1.3 Policy

1.3.1 Device Categories and Approved Usage

1.3.1.1 Company-Issued Devices (Primary Work Devices)

- **Laptops and Workstations**: All audit work, data analysis, and document creation
- **Security Management**: Implemented according to Asset / Device Management Policy (ASSETP)
- **Physical Security**: Must be locked when unattended and secured during travel

1.3.1.2 Personal Mobile Devices (Limited Business Use)

- **Approved Business Applications**:
  - Microsoft Outlook (email access only)
  - Microsoft Teams (communication and meetings)
- **Communication Functions Only**: Voice, email reading, calendar, instant messaging
- **Strict Prohibitions**:
  - No downloading or storing company/client documents
  - No screenshots of confidential information
  - No sharing documents to personal cloud services
  - No access to company WiFi networks

1.3.2 Security Requirements for Personal Devices

1.3.2.1 Mandatory Security Controls

- **Biometric Protection**: Fingerprint, face recognition, or minimum 6-digit PIN required

- **Auto-Lock**: Maximum 5-minute timeout for automatic screen lock
- **Operating System**: Must maintain current OS version with security updates
- **App Sources**: Only install apps from official stores (Apple App Store, Google Play)
- **Remote Wipe**: Consent to remote business data deletion if device is lost/stolen

1.3.2.2 Network and Access Restrictions

- **Public WiFi Usage**: Email/Teams access permitted but no client data access
- **VPN Requirements**: As specified in Acceptable Use Policy (AUP) for unsecured networks
- **Location Services**: May be required for business applications
- **International Travel**: Additional security protocols apply per destination

1.3.3 Data Protection Standards

1.3.3.1 Document and Information Handling

- **Email Attachments**: View-only access; client data processing and storage according to Information Governance and Data Stewardship Framework (DATAP)
- **Screenshots/Photos**: Capturing confidential information on personal devices forbidden
- **Cloud Storage**: No synchronization with personal cloud services (iCloud, Google Drive)
- **Offline Access**: Limited offline capabilities for approved applications only

1.3.3.2 Client Site Compliance

- **Client Security Policies**: Must comply with client's mobile device restrictions
- **Visitor Networks**: Use client-provided guest networks when available
- **Device Registration**: May require temporary registration with client security systems

1.4 Policy Review and Maintenance

This policy is subject to annual review and update by the System Administrator and Director.

1.5 Exceptions

All exceptions to this policy require written approval from the Director, accompanied by documented business justification and formal risk assessment. Approved exceptions include specific monitoring provisions and regular review schedules.

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 mandatory retraining, device access restrictions, formal reprimands, or termination of employment, depending on the nature and frequency of violations.

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.