Acceptable Use Policy

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.7, CC7.1

Table 2: Document history

Date	Comment
Oct 7 2024	Initial document
Nov 20 2024	Updated device usage policies

1 Acceptable Use Policy

Field	Value
ID	AUP-002
Effective Date	October 7, 2024
Last Revised	November 20, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Acceptable Use Policy establishes standards for authorized use of MMF Consulting Grp (Pte. Ltd.) information technology resources and defines prohibited activities. This policy applies to all employees, contractors, and third parties who access MMF Consulting Grp (Pte. Ltd.)'s IT systems, networks, data, and devices.

1.2 Background

MMF Consulting Grp (Pte. Ltd.)'s IT resources are provided to support business operations and client services. This policy ensures that technology use aligns with business objectives, protects confidential client data, and maintains system security and performance.

1.3 Policy

1.3.1 General Principles

All use of MMF Consulting Grp (Pte. Ltd.) IT resources must:

- Support authorized / legitimate business purposes
- Comply with applicable laws and regulations
- Protect confidential and proprietary information
- Maintain system security and integrity
- Respect intellectual property rights
- Follow professional standards and ethics

1.3.2 Acceptable Use

1.3.2.1 Authorized Business Activities

- Conducting compliance audits and contract reviews
- Analyzing client financial and sales data using approved tools (Excel, Power BI)
- Accessing client systems via approved VPN connections at vendor sites
- Professional communications via Microsoft 365 (Outlook, Teams)
- Training and professional development activities
- Accessing Box.com for secure document storage and collaboration
- Using personal mobile devices for Outlook/Teams communication only

1.3.2.2 Communication and Collaboration

- Use Microsoft Teams for internal meetings and client communications
- Access company email (Outlook) from approved devices only
- Share documents via Box.com secure links with proper access controls
- Use company-approved videoconferencing tools for client meetings

1.3.3 Prohibited Activities

1.3.3.1 Device and System Restrictions

- Personal use of company-issued laptops and workstations is prohibited
- Personal email access is not permitted on company devices
- Software installation requires explicit IT approval
- USB and removable media use requires explicit authorization
- Cloud services are limited to approved platforms (Box.com and Microsoft 365)

1.3.3.2 Data and Document Restrictions

- Printing confidential documents requires written approval
- Downloading client documents to personal mobile devices is prohibited
- Uploading data to non-approved cloud services (Dropbox, Google Drive, etc.) is prohibited
- Email forwarding of confidential information to personal accounts is prohibited
- Screenshot or photo capture of confidential information on personal devices is prohibited

1.3.3.3 Security and Access Violations

- Sharing login credentials or allowing unauthorized access is prohibited
- Bypassing security controls including VPN, MFA, or monitoring software is prohibited
- Connecting to unsecured WiFi without VPN protection (hotels, coffee shops) is prohibited
- Installing unauthorized remote access software is prohibited
- Disabling antivirus or security software (Microsoft Defender) is prohibited

1.3.3.4 Content and Conduct Restrictions

- Accessing inappropriate, illegal, or non-business websites is prohibited
- Downloading or distributing copyrighted material without authorization is prohibited
- Engaging in activities that could harm MMF Consulting Grp (Pte. Ltd.)'s reputation is prohibited
- Using systems for personal business ventures or competing activities is prohibited

1.4 Policy Review and Maintenance

This policy is subject to annual review and update:

- **Annual Review**: Conducted each November by the Director and HR/Legal Representative
- **Usage Monitoring**: Analysis of monitoring data and violation trends
- **Technology Changes**: Updates based on new applications and services
- **Employee Feedback**: Incorporation of user experience and practical considerations

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 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, system access restrictions, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Severe violations involving data breaches or malicious activity 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.