Asset / Device Management Policy

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, CC6.5

Table 2: Document history

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

1 Asset / Device Management Policy

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

1.1 Purpose and Scope

This Asset and Device Management Policy establishes requirements for identifying, tracking, securing, and managing all information technology assets owned or controlled by MMF Consulting Grp (Pte. Ltd.). This policy applies to all hardware, software, and digital assets used in business operations, including laptops, mobile devices, software licenses, and data storage systems.

1.2 Background

Effective asset management is critical for MMF Consulting Grp (Pte. Ltd.)'s security posture and compliance requirements. As a consulting firm handling sensitive client data across multiple engagements, proper asset tracking ensures appropriate security controls, license compliance, and rapid incident response. This policy supports audit requirements and enables effective risk management across all technology assets.

1.3 Policy

1.3.1 Asset Classification and Inventory

1.3.1.1 Hardware Assets

- **Company-Issued Laptops**: Primary work devices with full disk encryption and endpoint protection
- **Workstations**: Desktop computers in office environments with standardized security configurations
- **Mobile Devices**: Company-owned smartphones and tablets (if applicable)
- **Network Equipment**: Routers, switches, and networking hardware in office locations
- **Security Hardware**: Physical security devices, cameras, and access control systems
- **Peripherals**: Monitors, keyboards, mice, printers, and other attached devices

1.3.1.2 Software Assets

- **Operating Systems**: Windows licenses and management across all devices
- **Microsoft 365 Licenses**: User subscriptions, applications, and service components
- **Box.com Enterprise**: Storage licenses and user access permissions
- **Security Software**: Microsoft Defender for Business licenses and coverage
- **Productivity Applications**: Specialized audit and analysis software licenses
- **VPN Software**: Remote access solutions and client certificates

1.3.1.3 Digital Assets

- **Client Data**: Audit workpapers, financial data, contracts, and related documentation
- **Company Information**: Policies, procedures, employee records, and business documents

- **Intellectual Property**: Methodologies, templates, and proprietary analysis frameworks
- **System Configurations**: Security settings, user profiles, and administrative configurations

1.3.2 Asset Lifecycle Management

1.3.2.1 Procurement and Deployment

- **Standardized Hardware**: Approved laptop and workstation configurations with security requirements
- **Standard Operating System Builds**: All company-issued workstations must use official latest operating system builds with current security updates at time of deployment
- **Software Licensing**: Centralized procurement ensuring compliance with vendor terms
- **Security Configuration**: Mandatory security baseline applied before deployment
- **Asset Registration**: Addition to inventory database with owner assignment and classification
- **User Assignment**: Formal assignment process with acceptance of security responsibilities

1.3.2.2 Ongoing Management and Monitoring

- **Quarterly Inventory Reviews**: Physical verification and database updates
- **Security Patch Management**: Automated Windows Updates and monthly patch cycles
- **Software License Compliance**: Regular audits ensuring proper licensing for all installed software
- **Performance Monitoring**: Microsoft Defender for Business dashboards and health checks
- **Access Control Reviews**: Quarterly verification of user access and permissions

1.3.2.3 Maintenance and Support

- **Preventive Maintenance**: Regular system cleaning, updates, and performance optimization
- **Hardware Replacement**: Lifecycle management with 3-4 year replacement cycles
- **Warranty Management**: Tracking warranty status and coordinating repairs
- **Support Escalation**: Defined procedures for technical issues and vendor support
- **Emergency Replacement**: Rapid deployment procedures for critical system failures

1.3.2.4 Retirement and Disposal

- **Data Sanitization**: Complete data wiping using NIST-approved methods before disposal
- **Certified Destruction**: Physical destruction of devices containing irretrievable sensitive data
- **License Recovery**: Proper software license deactivation and reallocation
- **Environmental Disposal**: Responsible recycling through certified e-waste vendors
- **Documentation**: Disposal certificates and inventory database updates

1.3.3 Security Controls for Assets

1.3.3.1 Physical Security

- **Device Encryption**: BitLocker full disk encryption on all company laptops and workstations
- **Asset Tagging**: Physical identification tags with inventory numbers
- **Secure Storage**: Locked storage for spare equipment and sensitive devices
- **Transport Security**: Procedures for secure device transport between offices and client sites
- **Theft Reporting**: Immediate reporting and response procedures for lost or stolen assets

1.3.3.2 Logical Security

- **Endpoint Protection**: Microsoft Defender for Business on all devices
- **Administrative Restrictions**: Removal of local administrator privileges from standard users
- **Software Installation Controls**: Restriction of unauthorized software installation

- **Remote Management**: Centralized management through Microsoft Intune (if implemented)
- **Security Monitoring**: Continuous monitoring for threats and policy violations

1.3.3.3 Access Control Device access controls are managed in accordance with the Access Control Policy (ACP), including user authentication, multi-factor authentication requirements, and account lifecycle management.

1.3.4 Asset Tracking and Documentation

1.3.4.1 Inventory Database

- **Asset Details**: Serial numbers, models, purchase dates, warranty information
- **Assignment Records**: Current user, location, and usage classification
- **Configuration Data**: Security settings, software inventory, and patch status
- **Maintenance History**: Service records, repairs, and performance issues
- **Compliance Status**: License compliance, security policy adherence, and audit findings

1.3.4.2 Regular Reporting

- **Monthly Dashboards**: Asset health, security status, and compliance metrics
- **Quarterly Reviews**: Comprehensive asset verification and policy compliance assessment
- **Annual Audits**: Complete inventory validation and lifecycle planning
- **Exception Reporting**: Immediate notification of security issues or policy violations
- **Management Reporting**: Executive summaries of asset management effectiveness

1.3.5 Bring Your Own Device (BYOD) Management

Personal device usage is governed by the Mobile Device Policy (MOBP), which defines permitted applications, security requirements, and compliance monitoring procedures.

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. 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 asset access restrictions, mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Misuse of company assets or unauthorized asset disposal 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.