Information Security Policy

MMF Consulting Grp (Pte. Ltd.)

September 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.4, CC3.1, CC3.2, CC4.1, CC5.2, CC6.1, CC7.2, CC7.3

Table 2: Document history

Date	Comment
Sep 12 2024	Initial document
Nov 28 2024	Enhanced security controls

1 Information Security Policy

Field	Value
ID	ISP-002
Effective Date	September 12, 2024
Last Revised	November 28, 2024
Department	Information Security
Approval	Minny Wang, Director

1.1 Purpose and Scope

This Information Security Policy establishes the framework for protecting MMF Consulting Grp (Pte. Ltd.) information assets and client data. This policy applies to all employees, contractors, and third parties who access MMF Consulting Grp (Pte. Ltd.)'s information systems, regardless of location or device used.

The policy aims to:

- Protect the confidentiality, integrity, and availability of information assets
- Ensure compliance with legal, regulatory, and contractual requirements
- Minimize security risks to acceptable levels
- Establish clear accountability for information security

1.2 Background

As a compliance consulting and auditing firm handling sensitive client data including contracts, financial records, and vendor information, MMF Consulting Grp (Pte. Ltd.) recognizes that information security is critical to maintaining client trust and business operations. This policy establishes the foundation for our comprehensive security program aligned with industry best practices and regulatory requirements.

1.3 Policy

1.3.1 Information Security Program

MMF Consulting Grp (Pte. Ltd.) maintains a comprehensive information security program that includes:

1. **Governance and Oversight**
   - The Director maintains ultimate responsibility for information security
   - The System Administrator implements and monitors security controls
   - All employees are responsible for protecting information assets
2. **Risk Management**
   - Annual risk assessments identify and prioritize security threats
   - Risk mitigation strategies are implemented based on assessment results
   - Quarterly reviews ensure controls remain effective
3. **Asset Management**
   - Implementation according to Asset / Device Management Policy (ASSETP)
   - Regular inventories and lifecycle management procedures
4. **Access Control**
   - Implementation according to Identity and Access Management Framework (ACP)
   - Principle of least privilege and quarterly access reviews

5. **Data Protection**
    - Implementation according to Data Protection and Cryptographic Standards (ENCP) and Information Governance and Data Stewardship Framework (DATAP)
    - Mandatory encryption and client data segregation
6. **Security Monitoring**
    - Microsoft Defender for Business provides continuous threat monitoring
    - Security logs are reviewed weekly
    - Incidents are investigated and documented
    - Unsecure outbound connections are alerted / blocked to ensure encrypted data transfer
7. **Incident Response**
    - Security incidents are reported immediately to the System Administrator
    - Customer notifications occur within 72 hours when required
    - Post-incident reviews identify improvement opportunities
8. **Business Continuity**
    - Backup and recovery procedures as defined in Information Governance and Data Stewardship Framework (DATAP)
    - Recovery procedures are documented and tested annually
    - Alternative work arrangements ensure service continuity
9. **Compliance**
    - Adherence to US accounting regulations and CPA professional standards
    - Client contractual requirements are documented and tracked
    - Annual compliance reviews verify ongoing adherence
10. **Security Awareness**
    - Security training is conducted twice annually
    - Employees acknowledge security policies upon hiring
    - Regular communications reinforce security best practices

1.3.2 Roles and Responsibilities

Director (Minny Wang)

- Approve security policies and major changes
- Allocate resources for security initiatives
- Review and approve risk assessment results

System Administrator (Yusheng Li)

- Implement and maintain security controls
- Monitor security events and investigate incidents
- Conduct security training and awareness programs
- Perform quarterly reviews and assessments

HR/Legal Representative (Kelly Lee)

- Manage background checks and onboarding procedures
- Coordinate visitor access and physical security
- Support incident response and compliance activities

All Employees

- Comply with all security policies and procedures
- Report security incidents immediately
- Protect confidential information
- Complete required security training

1.3.3 Information Classification

All information must be classified according to the Data Classification Framework defined in Information Governance and Data Stewardship Framework (DATAP).

1.3.4 Acceptable Use

Information systems may only be used for authorized business purposes. Personal use is prohibited on company devices. Detailed requirements are specified in the Acceptable Use Policy (AUP).

1.3.5 Physical Security

Physical access to offices is controlled through keycards and monitored by security cameras. Visitors must sign in with HR/Legal. Clean desk policy is enforced in all work areas.

1.3.6 Remote Work Security

Employees working remotely must:

- Use company-issued devices with full disk encryption
- Connect through VPN when using public WiFi
- Maintain physical security of devices
- Follow all security policies regardless of location

1.3.7 Security Monitoring and Anomaly Detection

1.3.7.1 System Component Monitoring Continuous Monitoring Capabilities

- **Microsoft Defender for Business**: Real-time monitoring of all company devices for malware, suspicious activities, and security threats
- **Microsoft Entra ID**: Monitoring of authentication events, unusual login patterns, and access anomalies
- **Box.com Access Logs**: Tracking of file access, downloads, sharing activities, and unusual usage patterns
- **Network Traffic Monitoring**: Analysis of network communications for suspicious data transmission or unauthorized connections
- **Email Security**: Monitoring of email traffic for phishing attempts, malware attachments, and data exfiltration

Anomaly Detection Procedures

- **Automated Alerts**: Real-time notifications for suspicious activities including failed login attempts, unusual file access patterns, and potential malware infections
- **Behavioral Analysis**: Detection of deviations from normal user behavior patterns, including unusual working hours, geographic locations, or data access patterns
- **Threat Intelligence Integration**: Correlation of detected activities with known threat indicators and attack patterns
- **Performance Monitoring**: Detection of system performance anomalies that may indicate security compromises or resource abuse

1.3.7.2 Security Event Evaluation and Analysis Event Classification and Prioritization

- **Critical Events**: Immediate threat indicators requiring immediate response including malware detection, data exfiltration attempts, and unauthorized access
- **High Priority Events**: Significant security concerns requiring investigation within 4 hours (suspicious login patterns, policy violations, system vulnerabilities)

- **Medium Priority Events**: Potential security issues requiring review within 24 hours (configuration changes, unusual but authorized activities)
- **Informational Events**: Routine security events requiring periodic review (successful authentications, routine file access)

Investigation and Analysis Process

- **Initial Assessment**: System Administrator reviews all security alerts within defined timeframes based on priority level
- **Root Cause Analysis**: Detailed investigation of confirmed security events to determine cause, scope, and potential impact
- **Impact Evaluation**: Assessment of whether events could result in failure to meet business objectives or compromise client data
- **Evidence Collection**: Preservation of relevant logs, system states, and forensic evidence for further analysis
- **Escalation Procedures**: Director notification for events that may impact client data, business operations, or regulatory compliance

Response and Remediation Activities

- **Immediate Containment**: Isolation of affected systems, suspension of user accounts, or blocking of suspicious network traffic as appropriate
- **Threat Mitigation**: Implementation of additional controls or countermeasures to prevent similar incidents
- **System Recovery**: Restoration of normal operations while maintaining security integrity
- **Stakeholder Communication**: Notification of affected parties including clients, regulatory authorities, or law enforcement as required
- **Lessons Learned**: Documentation of incident details, response effectiveness, and recommendations for prevention of similar events

1.4 Compliance

This policy aligns with applicable regulatory requirements, professional standards, client contractual obligations, and industry best practices.

Non-compliance may result in disciplinary action up to and including termination.

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 Policy Review and Maintenance

This policy is subject to annual review and update to ensure continued effectiveness and compliance:

- **Annual Review**: Conducted each September by the Director and System Administrator
- **Interim Updates**: Policy may be updated as needed due to regulatory changes, security incidents, or business requirements
- **Stakeholder Input**: Employee feedback and audit findings are incorporated into reviews
- **Approval Process**: All changes require Director approval and employee acknowledgment
- **Version Control**: All revisions are documented in the majorRevisions section

1.7 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. The System Administrator investigates all violations and reports findings to the Director for appropriate action. Enforcement measures may include:

- **First offense**: Written warning and mandatory additional training
- **Second offense**: Formal disciplinary action and performance monitoring
- **Serious violations**: Immediate suspension or termination of employment

Severe violations involving data breaches, malicious activity, or deliberate security circumvention 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.