Data Protection and Cryptographic Standards

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 Data Protection and Cryptographic Standards

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

1.1 Purpose and Scope

This Data Protection and Cryptographic Standards policy establishes mandatory encryption requirements for protecting sensitive information at MMF Consulting Grp (Pte. Ltd.). This policy applies to all data storage, transmission, and processing activities involving confidential information, including client data, employee records, and proprietary business information across all systems and locations.

1.2 Background

Encryption is fundamental to MMF Consulting Grp (Pte. Ltd.)'s data protection strategy. As a compliance consulting firm handling sensitive client financial data, contracts, and audit documentation, robust cryptographic controls ensure confidentiality during storage, transmission, and processing. This policy leverages enterprise-grade encryption provided by Microsoft 365 and Box.com while establishing clear standards for all encryption activities.

1.3 Policy

1.3.1 Encryption Requirements by Data Classification

1.3.1.1 Confidential Data (Mandatory Encryption)

- **Client Financial Information**: Revenue data, cost structures, royalty calculations, financial analyses
- **Audit Documentation**: Workpapers, findings, client assessments, compliance reports
- **Contract Information**: Client agreements, vendor contracts, pricing terms, commercial arrangements
- **Personal Information**: Employee records, client contact data, identification information
- **Proprietary Methods**: Audit methodologies, analysis frameworks, intellectual property

1.3.1.2 Internal Data (Mandatory Encryption)

- **Business Documents**: Internal procedures, training materials, administrative records
- **Communication Records**: Email archives, meeting minutes, internal correspondence
- **System Documentation**: Configuration files, user guides, technical specifications

1.3.2 Encryption Standards and Algorithms

1.3.2.1 Approved Encryption Standards

- **Symmetric Encryption**: AES-256 (Advanced Encryption Standard with 256-bit keys)
- **Asymmetric Encryption**: RSA-2048 minimum, RSA-4096 preferred for key exchange
- **Hashing Algorithms**: SHA-256 minimum for data integrity verification

- **Transport Security**: TLS 1.2 minimum, TLS 1.3 preferred for data in transit
- **File Encryption**: AES-256 for individual file protection when required

1.3.2.2 Prohibited Encryption Methods

- **Deprecated Algorithms**: DES, 3DES, MD5, SHA-1, RC4
- **Weak Key Sizes**: RSA keys less than 2048 bits, symmetric keys less than 128 bits
- **Unvalidated Software**: Non-certified encryption tools or custom implementations
- **Export-Restricted Cryptography**: Algorithms prohibited by applicable export control laws

1.3.3 Data at Rest Encryption

1.3.3.1 Company Device Encryption

- **Full Disk Encryption**: BitLocker encryption mandatory on all company laptops and workstations
- **Encryption Key Management**: Windows-managed recovery keys stored in Microsoft Entra ID
- **USB/Removable Media**: BitLocker To Go required for any approved removable storage devices
- **Mobile Devices**: Hardware encryption enabled on all approved mobile devices
- **Backup Media**: Encrypted backup storage for any local backup devices

1.3.3.2 Cloud Storage Encryption

- **Box.com**: AES-256 encryption for all stored files with enterprise key management
- **Microsoft 365**: Customer-managed encryption keys where available for sensitive data, including OneDrive for Business, SharePoint collaboration spaces, and Exchange Online email storage
- **Client Data Protection**: All data must be encrypted at rest using AES-256 encryption minimum, ensuring no client information moves outside approved secure infrastructure without proper encryption

1.3.4 Data in Transit Encryption

1.3.4.1 Network Communications

- **Email Transmission**: TLS encryption for all email transmission
- **Web Communications**: HTTPS required for all web-based applications and services
- **File Transfers**: SFTP or HTTPS for secure file transmission to clients and vendors
- **VPN Connections**: IPSec or SSL VPN with strong encryption for remote access
- **API Communications**: TLS 1.2+ for all application programming interface connections
- **Client Data in Transit**: All client data (including Amazon data) must be encrypted in transit using TLS 1.2 minimum, with TLS 1.3 preferred for maximum security

1.3.4.2 Client Communications All client communications must use encryption methods specified in the Network Communications section above, with additional requirements for:

- **File Sharing**: Box.com secure links with password protection and expiration dates
- **Video Conferencing**: End-to-end encryption for confidential client meetings
- **Document Collaboration**: Encrypted channels for real-time document collaboration

1.3.5 Key Administration

1.3.5.1 Access Control for Encryption Systems

- **Administrative Access**: Restricted to System Administrator with documented procedures
- **Key Recovery**: Emergency key recovery procedures for business continuity
- **Audit Logging**: Comprehensive logging of all key management activities

- **Separation of Duties**: Multiple approvals required for sensitive key management operations
- **Third-Party Keys**: Secure management of encryption keys provided by clients or vendors

1.3.6 Compliance and Monitoring

1.3.6.1 Encryption Verification

- **Quarterly Audits**: Verification that all required encryption is properly implemented
- **Device Compliance**: Automated checking of BitLocker status on all company devices
- **Cloud Service Verification**: Regular confirmation of encryption settings in cloud services
- **Network Traffic Analysis**: Monitoring to ensure all sensitive data transmission is encrypted
- **Exception Reporting**: Immediate notification of any unencrypted sensitive data

1.3.6.2 Performance and Compatibility

- **Performance Testing**: Regular assessment of performance impact from encryption systems
- **Compatibility Verification**: Testing encryption compatibility with business applications
- **User Training**: Education on encryption requirements and proper usage procedures
- **Vendor Coordination**: Working with technology vendors to ensure encryption compliance
- **Update Management**: Coordinated updates of encryption software and configurations

1.3.7 Emergency Procedures and Business Continuity

1.3.7.1 Key Recovery and Disaster Response

- **Emergency Access**: Documented procedures for accessing encrypted data during emergencies
- **Key Recovery Time**: Target recovery time of 4 hours for critical business data
- **Backup Key Storage**: Secure offsite storage of key recovery information
- **Disaster Recovery Testing**: Annual testing of encryption key recovery procedures
- **Vendor Support**: 24/7 support agreements with encryption vendors for emergency situations

1.3.7.2 Incident Response for Encryption

- **Key Compromise**: Immediate key revocation and replacement procedures
- **Encryption Failure**: Response procedures for encryption system failures
- **Data Recovery**: Methods for recovering data when encryption keys are lost
- **Forensic Support**: Procedures for providing encrypted data to legal and forensic investigators
- **Client Notification**: Communication procedures for encryption-related incidents affecting client data

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 system access restrictions, mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Failure to encrypt sensitive data or circumventing encryption controls 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.