Information Governance and Data Stewardship Framework

MMF Consulting Grp (Pte. Ltd.)

October 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.1, C1.1, C1.2, A1.2

Table 2: Document history

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

1 Information Governance and Data Stewardship Framework

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

1.1 Purpose and Scope

This Information Governance and Data Stewardship Framework establishes comprehensive requirements for collecting, storing, processing, sharing, and disposing of information throughout its lifecycle at MMF Consulting Grp (Pte. Ltd.). This policy applies to all data types including client information, employee records, business documents, and system data across all storage locations and processing systems.

1.2 Background

As a compliance consulting firm, MMF Consulting Grp (Pte. Ltd.) handles vast amounts of sensitive client financial data, contracts, vendor information, and audit documentation. Proper data management ensures regulatory compliance, client confidentiality, business continuity, and legal protection. This policy aligns with US accounting regulations, client contractual requirements, and industry best practices for professional services firms.

1.3 Policy

1.3.1 Data Classification Framework

1.3.1.1 Classification Levels and Identification **Public Data** - **Definition**: Information that can be shared freely without risk to the organization or clients - **Examples**: Marketing materials, public filings, published reports, company website content - **Identification**: No special markings required - **Protection Requirements**: Standard business controls

Internal Data - **Definition**: Company information requiring basic protection from unauthorized disclosure - **Examples**: Internal policies, procedures, training materials, administrative documents - **Identification**: Header marking "INTERNAL USE ONLY" on documents - **Protection Requirements**: Access controls, secure storage, encrypted transmission

Confidential Data - **Definition**: Sensitive business and client information requiring strict access controls and encryption - **Examples**: Client financial data, contracts, audit workpapers, personal information, proprietary methods - **Identification**: Header marking "CONFIDENTIAL" with handling restrictions - **Protection Requirements**: Role-based access, encryption at rest and in transit, audit logging

1.3.1.2 Confidential Information Categories **Client Financial Information** - Revenue records, cost structures, royalty calculations, financial analyses - Contract pricing, commercial terms, vendor relationships - Must be maintained with strict confidentiality per client agreements

Audit and Compliance Documentation - Workpapers, findings, recommendations, compliance assessments - Investigation records, corrective action plans - Subject to 7-year retention requirement per US regulations

Personal and Sensitive Information - Employee records, client contact data, identification information - Health information, background check results - Subject to privacy regulations and contractual obligations

Proprietary Business Information - Audit methodologies, analysis frameworks, intellectual property - Client lists, pricing strategies, business development plans - Critical to competitive advantage and business operations

1.3.2 Data Lifecycle Management

1.3.2.1 Data Collection and Creation

- **Authorized Sources**: Client-provided data, public records, and authorized third-party sources
- **Collection Limitations**: Data collected only for legitimate business purposes and client engagements
- **Data Minimization**: Collect only information necessary for audit and compliance objectives
- **Client Consent**: Explicit agreements for data collection, processing, and retention
- **Source Documentation**: Maintain records of data sources and collection authorization

1.3.2.2 Data Storage and Organization

1.3.2.2.1 Primary Storage

- **Box.com Enterprise**: Primary cloud storage with enterprise-grade security and compliance features
- **Microsoft 365**: Email, collaboration documents, and integrated productivity tools
- **Local Device Storage**: Temporary storage on encrypted company laptops during audit fieldwork
- **Client Systems**: Temporary access during on-site audit procedures (no data retention)

1.3.2.2.2 Storage Requirements

- **Encryption Standards**: Data encryption requirements as specified in the Data Protection and Cryptographic Standards Policy (ENCP)
- **Access Controls**: Role-based permissions aligned with job responsibilities and client engagement needs
- **Geographic Restrictions**: Data stored in approved regions with adequate legal protections
- **Backup Systems**: Automated daily backups with versioning and disaster recovery capabilities
- **Client Segregation**: Separate folder structures and access controls for different client engagements

1.3.2.3 Data Processing and Analysis

- **Approved Tools**: Microsoft Excel, Power BI, and other authorized analysis applications
- **Processing Locations**: Company offices, approved remote work locations, and client sites
- **Data Transformation**: Documented procedures for data cleansing, aggregation, and analysis
- **Quality Controls**: Validation procedures ensuring data accuracy and completeness
- **Audit Trails**: Logging of all data processing activities and analytical procedures

1.3.2.4 Data Sharing and Transmission

- **Internal Sharing**: Secure collaboration through Box.com with appropriate access controls
- **Client Communications**: Encrypted email and secure file sharing through approved platforms
- **External Sharing**: Limited to authorized recipients with appropriate confidentiality agreements
- **International Transfers**: Compliance with applicable data protection regulations
- **Transmission Security**: TLS encryption for all data in transit

1.3.3 Data Retention and Disposal

1.3.3.1 Retention Requirements

- **Audit Workpapers**: 7-year retention per US accounting and regulatory requirements
- **Client Contracts**: Retained for contract term plus 7 years for potential disputes
- **Employee Records**: Maintained per applicable employment law requirements
- **Business Documents**: 3-year retention for general business records
- **System Logs**: 1-year retention for security and audit purposes

1.3.3.2 Retention Procedures

- **Automated Policies**: Box.com retention policies configured to enforce retention schedules
- **Annual Reviews**: Assessment of retention requirements and disposal eligibility
- **Legal Holds**: Suspension of disposal when litigation or investigation is anticipated
- **Client Requests**: Responsive deletion procedures for client data deletion requests
- **Documentation**: Detailed records of all retention and disposal activities

1.3.3.3 Confidential Information Disposal Procedures **Disposal Authorization** - **System Administrator**: Authorizes all electronic data disposal activities - **Director Approval**: Required for disposal of sensitive client data or audit workpapers - **Legal Review**: Verification that legal holds and retention requirements are met - **Client Notification**: Advance notice to clients when contractually required

Electronic Data Disposal Methods - **Cryptographic Wiping**: NIST 800-88 compliant secure erasure of electronic storage - **Physical Destruction**: Certified physical destruction of storage media when cryptographic wiping is insufficient - **Cloud Data Deletion**: Verified deletion from Box.com and Microsoft 365 with deletion certificates - **Backup Verification**: Confirmation that confidential data is removed from all backup systems and archives - **Mobile Device Wiping**: Remote wiping capabilities for company-issued mobile devices

Physical Document Disposal - **Certified Shredding**: Cross-cut shredding by certified document destruction services for confidential documents - **Witness Destruction**: System Administrator or designee witnesses destruction of highly sensitive materials - **Disposal Certificates**: Obtaining and retaining certificates of destruction from disposal vendors - **Secure Containers**: Locked disposal containers for confidential documents awaiting destruction

Disposal Documentation and Verification - **Disposal Logs**: Detailed records of what data was disposed, when, by whom, and using what method - **Verification Procedures**: Independent verification that disposal was completed according to policy - **Audit Trail**: Comprehensive documentation supporting compliance with retention and disposal requirements - **Exception Reporting**: Immediate escalation of any disposal failures or irregularities

1.3.4 Data Security and Privacy

1.3.4.1 Access Control Framework Data access controls are implemented in accordance with the Access Control Policy (ACP), including least privilege principles, role-based access, and quarterly access reviews.

1.3.4.2 Privacy Protection

- **Personal Information**: Enhanced protection for employee and client personal data
- **Anonymization**: Data de-identification when possible for analysis and reporting
- **Consent Management**: Documented consent for personal information processing
- **Individual Rights**: Procedures for data subject access, correction, and deletion requests
- **Cross-Border Transfers**: Adequate protection for international data sharing

1.3.4.3 Incident Response for Data Data breach and incident response procedures are defined in the Security Event Response and Recovery Plan (INCP), including breach notification, forensic investigation, and recovery procedures.

1.3.5 Data Quality and Integrity

1.3.5.1 Quality Assurance

- **Data Validation**: Verification procedures for accuracy, completeness, and consistency
- **Source Verification**: Cross-checking data against original sources and documentation
- **Version Control**: Management of document versions and change tracking
- **Error Correction**: Standardized procedures for identifying and correcting data errors
- **Quality Metrics**: Regular monitoring of data quality indicators and improvement initiatives

1.3.5.2 Backup and Recovery Infrastructure **Backup System Architecture** - **Cloud-Native Backups**: Box.com and Microsoft 365 provide automated, geographically distributed backups - **Local Backup Verification**: Weekly verification of cloud backup integrity and completeness - **Backup Encryption**: All backup data encrypted at rest using AES-256 encryption - **Geographic Distribution**: Backups stored across multiple geographic regions for disaster resilience - **Version Control**: Point-in-time recovery capabilities with retention of multiple file versions

Recovery Procedures and Testing - **Recovery Time Objectives (RTO)**: - Critical client data: 4 hours maximum - Business applications: 8 hours maximum - Non-critical systems: 24 hours maximum - **Recovery Point Objectives (RPO)**: - Client engagement data: 1 hour maximum data loss - General business data: 4 hours maximum data loss - **Monthly Recovery Testing**: Scheduled testing of backup restoration procedures for critical systems - **Annual Disaster Recovery Exercises**: Full-scale testing of complete system recovery capabilities

Environmental Protections and Monitoring - **Infrastructure Monitoring**: Continuous monitoring of cloud service availability and performance - **Automated Alerts**: Real-time notifications of backup failures or system anomalies - **Capacity Management**: Proactive monitoring of storage capacity and performance metrics - **Vendor SLA Management**: Ongoing assessment of cloud provider service level compliance - **Alternative Access Methods**: Multiple pathways for accessing critical business data during service disruptions

Recovery Infrastructure Design - **Redundant Systems**: Multiple cloud providers and access methods for critical business functions - **Data Replication**: Real-time synchronization between primary and backup systems - **Emergency Procedures**: Documented step-by-step recovery procedures for various failure scenarios - **Communication Plans**: Clear protocols for notifying stakeholders during recovery operations - **Business Impact Assessment**: Regular evaluation of recovery priorities and resource allocation

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 data access restrictions, mandatory retraining, formal reprimands, or termination of employment, depending on the nature and frequency of violations. Data breaches or unauthorized data disclosure 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.