Information Security Policy

mpac

1. Purpose and Objectives

This Policy establishes requirements to protect the Organization's information, systems, and assets. It ensures confidentiality, integrity, and availability of data and supports compliance with legal, regulatory, and contractual obligations.

2. Scope and Application

2.1 Definition of Information Security

Information security protects information and systems against unauthorized access, use, disclosure, modification, and disruption, ensuring confidentiality, integrity, and availability.

2.2 Approach to Information Security

Security is everyone's responsibility. The Organization adopts ISO 27001 practices to guide implementation and continuous improvement.

2.3 Structure of this Document

Controls are grouped into:

- Organizational
- People
- Physical
- Technological

3. Responsibilities

3.1 Employee

Employees are required to follow all relevant policies, complete information security training, and promptly report any policy violations to their manager.

3.2 Manager

Employees and managers are expected to follow all policy requirements, complete necessary security training, ensure accountability and competence among staff, enforce compliance, and address any policy violations within their areas of responsibility.

3.3 Department Head

Hold staff accountable for their policy responsibilities, ensure compliance among direct reports, contribute to policy updates, and address non-compliance within their area.

3.4 Director, Cyber Security

The Director of Cyber Security is responsible for investigating non-compliance issues in collaboration with relevant departments, monitoring and evaluating the effectiveness of the policy, recommending updates, providing guidance on policy interpretation and application, and supporting educational initiatives to ensure proper implementation and adherence to the policy.

3.5 Vice President & Chief Information Technology Officer

Oversee policy compliance reporting to senior leadership and ensure all employees are informed about the Policy.

3.6 President & Chief Administrative Officer

The President and Chief Administrative Officer is responsible for ensuring direct reports adhere to the Policy, approving the Policy and any amendments, and addressing non-compliance issues in alignment with this and other applicable Corporate Policies.

3.7 Vendor / Third-Party Providers

Vendors and third-party providers must protect organizational data, enforce security measures as defined by policy and contracts, report incidents involving MAPC or MPAC data without delay, and ensure their subcontractors uphold equivalent or stronger security controls.

4. References

ISO 27001, ISO 27002, NIST Cybersecurity Framework, and Cloud Security Alliance (CSA) guidance.

5. Organizational Controls

5.1 Policies for Information Security

5.1.1 The Organization develops, shares, and communicates its approved information security policies and standards with employees and relevant external groups. These policies and standards are regularly evaluated for their appropriateness, completeness, potential improvements, and effectiveness, especially at scheduled times or after major changes occur. Information security controls are put in place throughout the organization to uphold these policies.

5.2 Information Security Roles and Responsibilities

5.2.1 The Organization designates roles and responsibilities. It oversees key information security processes. Data owners provide resources and put security controls in place. While data owners can delegate tasks, they stay accountable for them.

5.3 Segregation of Duties

5.3.1 The purpose of segregation of duties is to lower the risk of fraud, errors, and the circumvention of security controls. This is achieved by ensuring that conflicting duties are managed by different individuals, establishing clear processes for granting and elevating access, and separating conflicting roles whenever feasible.

5.4 Management Responsibilities

5.4.1 Management is tasked with ensuring that employees, contractors, and consultants understand and uphold their information security responsibilities. The organization clearly communicates these responsibilities to new staff, provides comprehensive training on information security policies, and keeps personnel informed of significant policy updates. Additionally, ongoing refresher training is delivered to all employees to address current threats and any substantial changes to the information security framework.

5.5 External Authorities & Special Interest Groups

5.5.1 The organization ensures robust communication regarding information security with legal, regulatory, and supervisory authorities by establishing clear processes and maintaining appropriate contacts.

5.5.2 It also actively participates in special interest groups and forums to stay current on best practices, receive timely warnings about threats and vulnerabilities, and enhance incident response capabilities through established liaison channels.

5.6 Threat Intelligence

5.6.1 The organization aims to enhance awareness of its threat environment, enabling effective mitigation and prevention of threats to reduce their impact.

5.7 Information Security in Project Management

5.7.1 Project management must address information security risks throughout the project life cycle by assessing risks early, including security requirements from the start, and identifying necessary controls promptly.

5.8 Inventory of Information and Associated Assets

5.8.1 The organization maintains an inventory of information and related assets, assigns ownership for security, and documents asset details to ensure protection and accountability.

5.9 Acceptable Use

5.9.1 The organization establishes clear rules and procedures to ensure the proper and secure use and handling of information and technology assets.

5.10 Return of Assets

5.10.1 The organization should clearly identify and document all information and other associated assets to be returned.

5.11 Information Classification & Labelling

5.11.1 Information must be classified and labelled to ensure it receives suitable protection based on its importance to the organization.

5.11.2 Owners are responsible for classification, which considers confidentiality, integrity, and availability, and is determined by the potential impact of compromise.

5.12 Information Transfer

5.12.1 The section outlines the need to ensure secure transfer of information both within the organization and with external parties, emphasizing formal agreements, protection of electronic messages, and maintaining information residency in Canada.

5.13 Access & Identity Management

5.13.1 Authentication information must be allocated formally, with users responsible for protecting it and using strong passwords.

5.13.2 Access rights should be managed through formal processes, reviewed regularly, and revoked or adjusted after employment changes.

5.13.3 For suppliers, security requirements should be documented and processes implemented to address risks related to supplier access and products.

5.14 Supplier, Cloud, and ICT Supply Chain Security

5.14.1 The organization must establish and document clear information security requirements within all supplier relationships, including agreements and ICT supply chain arrangements.

5.14.2 This involves identifying and mitigating risks, setting and monitoring service levels, and ensuring that both parties understand their security obligations.

5.14.3 For cloud services, the organization should implement and share relevant security policies with stakeholders.

5.15 Incident Management

5.15.1 Organizations must establish clear procedures for managing security incidents, including defined roles and reporting processes. Incidents should be categorized and prioritized, with effective response plans communicated to all stakeholders. Lessons learned from incidents should inform future improvements. Proper evidence collection procedures are essential for legal and disciplinary actions.

5.16 Business Continuity & ICT Readiness

5.16.1 Information security and ICT readiness during disruptions focus on protecting organizational assets and ensuring availability. Security controls should be adapted and integrated into business continuity plans, with ICT readiness supporting ongoing operations even when disruptions occur.

5.17 Compliance, IP, Records, and Privacy

5.17.1 The organization must comply with legal, regulatory, and contractual obligations regarding information security, intellectual property, and records management.

5.17.2 It protects records and personally identifiable information (PII) from unauthorized access, loss, and misuse, and implements necessary controls and measures to safeguard privacy and proprietary products.

5.18 Independent Review & Operating Procedures

5.18.1 The organization ensures information security by conducting regular independent reviews, maintaining compliance with established policies and standards, and documenting accessible operating procedures for information processing.

6. People Controls

6.1 Screening

6.1.1 Screening ensures all personnel are suitable and aware of their responsibilities. The organization conducts integrity and ethics checks, collecting candidate information in line with relevant laws.

6.2 Terms and Conditions of Employment

6.2.1 All personnel must be informed of their information security responsibilities both before and upon employment.

6.3 Security Awareness, Education, and Training

6.3.1 All personnel and relevant parties must regularly receive training and updates on information security responsibilities, current threats, policy changes, and, for technical teams, tailored skill development. Training occurs periodically and is refreshed as needed.

6.4 Disciplinary Process

6.4.1 The disciplinary process ensures everyone understands the consequences of violating information security policies. Disciplinary actions are only taken after confirming a violation, and responses consider legal and business requirements. The process serves both as a deterrent and a means to address violations, with immediate action possible for deliberate breaches

6.5 Responsibilities After Termination

6.5.1 The process for managing termination or change of employment should define which information security responsibilities and duties should remain valid after termination or change.

6.6 Confidentiality or Non-Disclosure Agreements

6.6.1 Agreements must ensure the protection of confidential information for both personnel and external parties. These agreements should be periodically reviewed and updated as needed.

6.7 Remote Working

6.7.1 Remote working refers to personnel accessing organizational information from outside official premises, including “teleworking”, “telecommuting”, “flexible workplace”, “virtual environments”, and “remote maintenance”. The purpose is to maintain information security during such work arrangements.

6.8 Information Security Event Reporting

6.8.1 Ensure prompt and effective reporting of information security events by all personnel to prevent or reduce incident impacts.

7. Physical Controls

7.1 Physical Security & Monitoring

7.1.1 Physical Security Perimeters: Define and regularly test security boundaries to prevent unauthorized access, damage, or interference.

7.1.2 Physical Entry: Control all access points, especially delivery and loading areas, to restrict entry to authorized individuals only.

7.1.3 Securing Offices, Rooms, and Facilities: Implement physical controls to safeguard organizational assets from unauthorized access or harm.

7.1.4 Physical Security Monitoring: Use surveillance systems such as guards, alarms, CCTV, or security management software to monitor and deter unauthorized access.

7.2 Protecting Against Physical and Environmental Threats

7.2.1 The organization must identify and manage risks from physical and environmental threats (e.g., fire, flood, earthquake, civil unrest, toxic waste), put safeguards in place, monitor changes, and seek expert advice when needed.

7.3 Secure Areas

7.3.1 The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

7.4 Clear Desk and Clear Screen

7.4.1 The organization should establish and communicate a standard on clear desk and clear screen to all relevant interested parties.

7.5 Equipment & Media Protection

7.5.1 The sections outline the need for guidelines to protect equipment from physical and environmental threats, secure organization assets used off-premises with management authorization, and manage and securely dispose of storage media to prevent unauthorized access or information loss.

7.6 Utilities, Cabling, Maintenance, and Disposal

7.6.1 This section outlines formal guidelines to safeguard organizational assets and information from risks associated with utility failures, cabling issues, equipment maintenance lapses, and improper disposal or re-use of equipment.

7.6.2 It emphasizes protecting supporting utilities (e.g., electricity, telecommunications), securing power and communication cabling, maintaining equipment with appropriate controls, and ensuring secure disposal or re-use of devices to prevent information leakage.

8. Technological Controls

8.1 User Endpoint Devices

8.1.1 User Endpoint Devices: Establish and communicate secure configuration standards for user devices, ensuring all users understand and follow security procedures.

8.2 Privileged Access & Source Code Control

8.2.1 Privileged access rights and information access must be strictly controlled to ensure only authorized users, components, and services receive necessary permissions.

8.2.2 The organization should implement standards for access control and information access, preventing unauthorized use of assets.

8.2.3 Additionally, access to source code and related development tools should be tightly restricted to maintain confidentiality and prevent unauthorized changes.

8.3 Secure Authentication

8.3.1 Ensure users and entities are properly authenticated when accessing systems. Use suitable authentication methods based on the sensitivity of the information, with stronger techniques (e.g., biometrics, tokens) for higher-risk access.

8.4 Capacity Management

8.4.1 Ensure that all information processing facilities, human resources, and offices have sufficient capacity to meet business needs. Identify requirements based on system and process criticality.

8.5 Protection Against Malware

8.5.1 Protection Against Malware ensures the organization implements controls and user awareness to detect, prevent, and respond to malware threats, minimizing the risk of malicious software affecting information assets.

8.6 Technical Vulnerabilities

8.6.1 The organization aims to prevent exploitation of technical vulnerabilities by: applying necessary patches, avoiding vendor default passwords, conducting regular internal vulnerability scans on systems handling confidential data, and using trusted third parties for external scans of publicly accessible systems.

8.7 Configuration Management

8.7.1 Configuration Management ensures that all hardware, software, services, and networks operate securely and as intended, by enforcing approved configurations and controlling any changes through defined roles and procedures.

8.8 Data Deletion, Masking, and Leakage Prevention

8.8.1 The organization ensures sensitive information is deleted when no longer needed, limits exposure of personal data through masking or anonymization, and monitors for data leaks to prevent unauthorized disclosure.

mpac

8.9 Information Backup

8.9.1 Establishes and tests backup and recovery strategies to ensure data and system restoration in case of loss.

8.10 Redundancy

8.10.1 The Organization evaluates the need for and, if required, accordingly maintains redundant information processing facility to sufficiently meet the Organization's availability requirements.

8.11 Logging & Monitoring

8.11.1 The Organization records and protects log data, monitors systems for security events, complies with legal requirements, and retains logs as required.

8.11.2 The Organization regularly monitors information systems to detect security incidents and assess the effectiveness of controls.

8.12 Clock Synchronization

8.12.1 The Organization must synchronize all key system clocks to a single time source.

8.13 Utility Programs & Software Installation

8.13.1 Only authorized personnel may use privileged utility programs, which must be identified and cannot bypass security controls.

8.13.2 Software changes and installations must follow secure guidelines, with only approved applications allowed and dependencies kept updated.

8.14 Network Security, Services, Segregation & Web Filtering

8.14.1 Organizations must implement strict controls to safeguard information and infrastructure from network threats and unauthorized access.

8.14.1 This includes securing network services, segregating networks for security boundaries, and managing access to external websites to prevent malware and unauthorized use.

8.15 Use of Cryptography

8.15.1 Cryptography is used to ensure information remains confidential, authentic, and intact. The organization evaluates when cryptography is appropriate, restricts use to approved methods, and manages cryptographic keys securely throughout their lifecycle.

8.16 Secure Development Lifecycle

8.16.1 Implement security controls throughout all stages of software and system development, including establishing formal rules and securing.

8.16.2 Identify and address security requirements during application development or acquisition.

8.16.3 Apply security principles to system.

8.16.4 Enforce organization-wide secure coding standards for all new and reused software. Integrate security testing at each development phase and verify systems before production deployment.

8.16.5 Clearly communicate and monitor security requirements with external development partners.

8.16.6 Maintain strict separation between development, test, and production environments to protect production data.

8.16.7 Require formal approval and testing for all production changes to ensure security is maintained.

8.16.8 Avoid using live production data for testing; if unavoidable, anonymize or alter data to protect privacy.

8.16.9 Coordinate and control audit activities to minimize operational impact and restrict access to audit tools.

9. Policy Compliance

9.1 Exceptions

Require formal approval and documented risk acceptance.

9.2 Non-Compliance

May result in disciplinary action, up to termination.

10. Definitions

Information: Knowledge communicated or received. Information in all forms (such as text, image, video and voice), in all media (such as paper, magnetic tape, disks, microfilm/microfiche) and at all stages of lifecycle (i.e., created, entered, processed, communicated, transported, disseminated, stored or disposed of) including the description of the information contents, origins, structure and relationships enabling correct interpretation of information. Forms and media for information include current and future technologies.

Information System: A combination of people, information technology hardware, software, services and automated or non-automated processes that have been organized to accomplish MPAC objectives.

ISMS: ISMS stand for Information Security Management System. It's a systematic approach to manage and protect MPAC data.

Risk assessment: The process of identifying and evaluating risks relevant to MPAC.

Data classification: The process of categorizing data based on its level of sensitivity and the impact to MPAC should that data be disclosed, altered, or destroyed without authorization.

Vulnerability: Vulnerability is a weakness in computer systems which can be exploited by attacker.

Security incidents: Any incident involving the actual or suspected loss, theft, misuse, unavailability of, or unauthorized access, acquisition, use, disclosure, modification, or destruction, or other compromise of, MPAC Data.

Business applications: A computer program designed to accomplish MPAC objectives.

An application can be developed by MPAC internally or can be purchased from a third party.

Business Continuity Management: The program and activities associated with developing and maintaining Business Continuity Plans.