MFEC

Information Security Policy

Version 2.0

Information Security Policy

As MFEC Public Company Limited (MFEC) has implemented information systems to support its operations and provide services to both internal and external users, it is essential to ensure that the use of information and information technology systems is appropriate, efficient, secure, and able to operate continuously. This also includes preventing potential problems arising from improper use or threats, which may cause risks affecting business operations, assets, and personnel.

Information security refers to safeguarding the confidentiality, integrity, and availability of MFEC's information and information technology systems. This means ensuring that information and systems are not disclosed to unauthorized individuals (Confidentiality), maintaining the accuracy and completeness of information (Integrity), and ensuring that authorized users can access and use the information as required (Availability).

Accordingly, MFEC establishes its Information Security Policy, including policies, guidelines, standards, and procedures, in written form. These are aligned with applicable laws, standards, and international best practices in information security.

Details and the structure of the Information Security Policy are provided in the annexed document: *Components and Structure of the Information Security Policy*.

Objectives of Information Security

1. To establish and announce policies, guidelines, standards, and procedures for executives, staff, system administrators, and external parties working with MFEC, in order to raise awareness of the importance of information security and to ensure proper compliance.
2. To ensure confidence in MFEC's information security that it is accessible only by authorized individuals (Confidentiality), accurate and complete (Integrity), and available for use (Availability).
3. To develop a systematic information security management process that is continuously improved and enhanced.
4. To comply with regulations, contractual requirements, and laws related to information technology security.

Approach

Information Security Practices (Reference Document: MFEC-ISMS-PO-002)

1. Conduct studies, development, and documentation of organizational context, stakeholder requirements, and the definition of information security scope to serve as the foundation for implementation.
2. Establish a standard information security framework to provide a clear operational model.

3. Ensure top management involvement, including the establishment of the information security policy, as well as defining clear roles and responsibilities of personnel related to information security.
4. Define information security objectives and integrate them with risk assessment results in order to prepare the annual information security plan.
5. Ensure adequate support in terms of resources, capability development, personnel awareness, communication throughout the process, and documentation to achieve the objectives of information security.
6. Monitor information security projects and processes to ensure alignment with planned objectives.
7. Evaluate the effectiveness of information security implementation across various dimensions, including policies, personnel awareness, operational processes, legal compliance, and information technology.
8. Conduct independent reviews of information security practices to ensure transparency and effectiveness in implementation.
9. Prepare and submit performance reports to management for acknowledgment and decision-making in order to improve the efficiency and effectiveness of information security operations.

1. Access Control Sub-Policy

MFEC Public Company Limited (MFEC) implements controls over the use and access to information and information systems. The objective is to establish measures that prevent unauthorized access to information and systems, protect against intrusion through physical, network, or software means that may cause data damage or system disruption, and ensure proper monitoring and verification of individuals accessing organizational information or systems. The policy is based on the following principles:

Confidentiality – Ensuring that only authorized individuals can access information, and that confidential data is protected from unauthorized disclosure.
Integrity – Ensuring the accuracy and completeness of information, while preventing errors, unauthorized modification, deletion, or alteration.
Availability – Ensuring that only authorized users can access information at agreed times, maintaining system continuity and performance, and preventing disruptions or downtime.

Objectives of Access Control

1. To establish guidelines, standards, and procedures for executives, staff, system administrators, and external parties working with MFEC, ensuring awareness of the importance of proper use and access to information and systems.

2. To build confidence in MFEC's information security by ensuring that information is accessible only by authorized personnel (Confidentiality), accurate and complete (Integrity), and available for use (Availability).
3. To enable audit trails for user access to information systems.

Approach

1. Establish written guidelines and procedures for the use and access of information and systems, aligned with applicable laws, principles, and international information security standards.
2. Ensure that information, IT systems, IT equipment, facilities, environments, system development, and maintenance are adequately protected with clear access control measures based on operational and security requirements.
3. Define access control practices for software development, including data access permissions within systems, as well as operating system-level access control covering various data areas within user computers.
4. Establish access control procedures for computers and IT equipment.
5. Establish access control procedures for server rooms, data centers, and IT infrastructure to ensure that only authorized personnel are granted access.
6. Ensure that all users are informed and trained regarding policies, standards, guidelines, rules, and procedures for using information and systems, and that they strictly comply with them.

Scope of the Access Control Sub-Policy

The scope of this sub-policy covers access to information, information systems, IT systems, server rooms, networks, and IT equipment. Information refers to both electronic and non-electronic formats.

2. Data Classification Sub-Policy

MFEC Public Company Limited (MFEC) establishes a data classification policy to ensure that information users and information owners are aware of the proper practices for handling information. This facilitates the application of appropriate information management methods in alignment with the principles of Confidentiality, Integrity, and Availability.

Objectives of Data Classification

1. To establish guidelines, standards, and procedures for executives, staff, system administrators, and external parties working with MFEC, ensuring awareness of the importance of safeguarding and maintaining information throughout its lifecycle—from creation, use, to retirement.

2. To build confidence in MFEC's information security by ensuring that information is accessible only by authorized personnel (Confidentiality), accurate and complete (Integrity), and available for use (Availability).
3. To raise employee awareness regarding information security.

Approach

1. Establish written guidelines and procedures for the use and access of information and systems, in alignment with applicable laws, principles, and international information security standards.
2. Ensure that all users are informed and trained regarding policies, standards, guidelines, rules, and procedures for handling and using information and systems, and require strict compliance.

Scope of the Data Classification Sub-Policy

The scope of this sub-policy covers the definition of practices for different types of information throughout their lifecycle—creation or acquisition, use, duplication, distribution, retirement, or destruction. This applies to both electronic and non-electronic forms of information.

3. Sub Policy for Operation Security

MFEC Public Company Limited (MFEC) has established this policy to ensure that daily operations are adequate, correct, appropriate, and secure, in accordance with the standards of Confidentiality, Integrity, and Availability.

Objectives of Operation Security

1. To define practices, requirements, and procedures for executives, staff, system administrators, and external parties working for MFEC to understand the necessary activities in operating with information and information systems.
2. To ensure confidence in preventive measures and recovery when problems occur with information or information systems.
3. To provide executives with proper and sufficient reports for information security management.

Guidelines

1. Establish documented practices and procedures for the use and access of information and information systems, in compliance with laws, principles, and international standards of information security.
2. Provide users with knowledge about policies, requirements, practices, regulations, and procedures related to the use of information and information systems, with strict adherence required.

Scope of the Sub Policy for Operation Security

The scope of the Sub Policy for Operation Security refers to the determination of practices for various necessary operations to build confidence in the use of information and information technology systems.

4. Communication Security Sub-Policy

MFEC Public Company Limited (MFEC) has established this policy to ensure the security of communication both within and outside the organization in accordance with the standards of confidentiality, integrity, and availability.

Objectives of Communication Security

1. To define the guidelines, requirements, and procedures for executives, officers, system administrators, and external personnel working for MFEC to be aware of the necessary activities in managing information communication.
2. To create confidence in secure management of information exchange from a preventive perspective.
3. To provide information system users with confidence in communicating information within the communication system both internally and externally.

Guidelines

1. To provide documented guidelines and procedures regarding the use and access of information and information systems, in compliance with laws, principles, and international standards of information security.
2. To ensure that users are provided with knowledge about policies, requirements, guidelines, regulations, and procedures related to the use of information and information systems, and that users strictly adhere to and comply with them.

Scope of the Communication Security Sub-Policy

The scope of the Communication Security Sub-Policy refers to the establishment of operational guidelines necessary to ensure confidence in the use of information and information technology systems.

5. Sub-Policy on Information Technology System Continuity Management

Since MFEC Public Company Limited (MFEC) has established preventive guidelines and preparedness measures for managing crisis situations in order to ensure that MFEC can continue its operations without interruption, the company has therefore defined a sub-policy on Information Technology System Continuity Management. This is to enable timely response and mitigate the impact on critical

business processes that depend on information technology systems, ensuring that they can continue operating at the level agreed upon with stakeholders.

Objectives of Information Technology System Continuity Management

1. To conduct analysis, planning, preparation, review, and simulation of necessary processes.
2. To ensure the continuous operation of information systems at the agreed level during emergency situations.
3. To ensure stakeholders have a mutual understanding and are aware of their roles and responsibilities in the event of an emergency or incident.

Guidelines

Information Technology System Continuity Management refers to the preparation of backup processes or systems to be utilized as substitutes when the primary system suffers disruption during emergencies, at the level already agreed upon. This shall be in accordance with the conditions defined through Business Impact Analysis (BIA), Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO), as well as to restore the main system back to normal operations.

MFEC has therefore established a sub-policy on Information Technology System Continuity Management that includes written policies, guidelines, standards, and procedures, in accordance with legal requirements, best practices, and international standards for IT continuity management, as follows

1. Establish an Information Technology System Continuity Management working group aligned with MFEC's overall business continuity management framework, including planning, implementation, drills, and continuous improvement.
2. Collaborate with the Risk Management Committee and the Internal Control Subcommittee, which oversee the overall development of MFEC's business continuity management system.
3. Collaborate with security-related departments to ensure integration between different scopes that rely on information systems, in preparing emergency prevention/response plans, and participate in the structure of the Emergency Operations and Crisis Management Center.
4. Develop an Information Technology System Continuity Management system within the responsible scope, including planning, implementation, drills, and continuous improvement, as well as assign responsible persons to develop plans to protect critical IT infrastructure. Regularly report the performance results to the Risk Management and Internal Control Committee, or when significant changes occur.

5. Ensure that executives/managers are responsible for driving and supporting operations in accordance with the IT system continuity management process, as well as enhancing the knowledge and capabilities of relevant personnel to ensure they can work effectively.

Ensure that executives, staff, employees, contractors, and related parties receive the necessary knowledge and awareness to participate in achieving the objectives of MFEC's business continuity management for information technology systems.

Scope of the Sub-Policy on Information Technology System Continuity Management

The scope of processes, services, workplaces, IT system continuity requirements, as well as information services that support critical processes to be included within the scope of this policy, can be determined from factors of significance, focusing on processes that rely on information systems, as follows:

- Critical business processes that rely on information systems, including the Project Management System, Accounting, Finance, and Payment System, Document Storage and Electronic Document Management System, and the organization's main website.
- The level of importance for IT system recovery.
- Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO).
- Requirements relating to timeframes in processes such as contract execution, financial and accounting disbursements, and project implementation.
- Requirements of the Information Technology Department in its role as the provider of essential IT services to the organization, including provision of information systems, computers, and networking equipment.
- Significant risks at main operational sites that may impact the delivery of essential systems and services, such as server rooms and network equipment facilities within the organization.
- Significant risks arising from reliance on technology services from a single service provider.

6. Sub-Policy on Risk Management for Information Security

Risks can arise from various factors and in various forms, and the use of information technology as a tool for operations may introduce risks to the organization. Key risks of concern include access risk (unauthorized access to data and computer systems) and infrastructure risk (inadequate or inappropriate management of computer systems or IT personnel). Such risks can have negative impacts on the organization and its partners, and thus regular risk assessments

are required to ensure proper risk management. This will strengthen the stability of the information system, ensuring that the organization's systems are available, uninterrupted, and secure.

Objectives

1. To inspect and assess risks to the information system, or identify undesirable or unpredictable information security situations.
2. To consider preventive measures and reduce potential risks to the information system.
3. To provide guidelines for response in the event of risks that threaten the information system.
4. To ensure that the organization's information storage complies with information security and personal data protection policies and regulations.
5. To align with MFEC's risk management framework.

Guidelines

1. The organization shall conduct an information security audit and assessment of the information systems at least once a year.
   1.1 Approval shall be obtained to proceed with information security risk assessments.
   1.2 Findings and recommendations from the risk assessment shall be documented in a report.
   1.3 Risk assessments shall be carried out by MFEC's Internal Auditor or an independent external information security auditor at least once a year.
2. Risk assessments and audits shall be conducted either by internal auditors or external independent information security auditors in order for the organization to understand its risk level and information security maturity.
   2.1 The information security policy, operations, procedures, and related processes shall be reviewed and updated to ensure alignment with policy requirements.
3. At least once a year, the fund manager shall be informed of findings, along with recommendations for improvements, where deficiencies in the IT security system are identified.
   3.1 Especially for critical and high-risk systems, regular security testing (e.g., penetration testing) shall be performed to identify vulnerabilities and evaluate the effectiveness of security controls.
   3.2 Tools for auditing the entire computer system—including software, applications, and necessary documentation—must be protected against unauthorized use or misuse, and access shall be restricted to audit-related departments only.

4. Risks from access to information or devices used for information processing by individuals or external parties shall be assessed.
5. Measures for information system audit and assessment shall include:
   5.1 Establishing agreements between auditors and system administrators and/or system owners.
   5.2 Creating copies of data for audit purposes, ensuring that these are destroyed immediately after the audit is completed or securely stored with appropriate protection measures if not destroyed.
   5.3 Granting auditors read-only access to data.
   5.4 Establishing secure storage methods for audit evidence.
   5.5 Defining clear procedures and responsibilities for auditors.
6. Personnel serving as auditors shall be independent from the activities or IT systems being audited.
7. Risk assessment results shall be presented in the form of a risk map, in accordance with MFEC's risk management framework.

7. Sub-Policy on Supplier Management

MFEC Public Company Limited (MFEC) has established this policy to ensure effective management of resources from both internal and external suppliers, starting from risk analysis to managing risks related to suppliers that could impact information and information technology systems.

Objectives of Secure Operations

1. To establish practices, requirements, and procedures for executives, staff, system administrators, and external parties working with MFEC to understand the necessary activities when receiving services from both internal and external suppliers.
2. To build confidence in the support and problem resolution of IT systems provided by external suppliers, including vendors or manufacturers.
3. To ensure readiness in mitigating risks that may arise from both internal and external suppliers.

Guidelines

1. Assess risks associated with all internal and external suppliers to determine measures for resolving and mitigating such risks.
2. Establish documented practices and procedures for supplier management in accordance with applicable laws, principles, and international standards for information security.
3. Ensure that all relevant parties are aware of the practices and procedures for supplier management and can carry them out appropriately.

4. Monitor and verify the operations and practices of relevant parties to ensure compliance with the intended direction.

Scope of the Sub-Policy on Supplier Management

The scope of this sub-policy covers the management of both internal and external suppliers through agreements and contracts signed by authorized representatives from both parties.

8. Sub-Policy on System Acquisition and Development

MFEC Public Company Limited (MFEC) has established this policy to ensure that the acquisition and development of systems are secure, operate smoothly, and do not negatively affect business operations.

Objectives of Secure Operations

1. To establish practices, requirements, and procedures for executives, staff, system administrators, and external parties working with MFEC to understand the necessary activities in system acquisition and system development.
2. To build confidence that the acquired or developed systems can operate effectively.
3. To reduce the number of complaints and issues arising from inefficient systems.

Guidelines

1. Establish documented practices and procedures for managing system acquisition and development in compliance with applicable laws, principles, and international standards for information security.
2. Ensure that all relevant parties are informed of the practices and procedures for managing system acquisition and development.
3. Implement the policies and guidelines defined to ensure confidence in the efficient acceptance and commissioning of systems.

Scope of the Sub-Policy on System Acquisition and Development

This sub-policy covers the management of information technology systems located in the primary data center and disaster recovery data center, as well as processes involving stakeholders in the acquisition and development of systems.

9. Sub-Policy on Human Resource Management Related to Information Security

MFEC Public Company Limited (MFEC) has established this policy to ensure that company personnel understand their roles and responsibilities, and to reduce the risks of theft, fraud, and misuse of company equipment.

Objectives of Secure Operations

1. To establish practices, requirements, and procedures for executives, staff, system administrators, and external parties working with MFEC to understand the necessary activities in human resource management.
2. To acquire qualified personnel and to develop existing personnel to align with the company's operational direction.
3. To reduce the risks of information leakage caused by internal company personnel.

Guidelines

1. Establish documented practices and procedures for human resource management in compliance with applicable laws, principles, and international standards for information security.
2. Ensure that all relevant parties are informed of the practices and procedures for human resource management.
3. Implement the policies and guidelines defined to ensure that existing personnel can perform their work in response to business needs effectively.

Scope of the Sub-Policy on Human Resource Management

The scope of this sub-policy covers both internal personnel and external stakeholders, such as outsourced staff or third parties, who are required to comply with the human resource measures defined herein.

10.Policy on Bringing Your Own Device (BYOD Policy)

This policy aims to establish understanding and provide operational guidelines regarding the use of personal devices within the network system of MFEC Public Company Limited, under the supervision of the IT Support department. The details are as follows:

Objectives

1. To improve work efficiency by allowing the use of devices that meet the employee's needs.
2. To increase flexibility and convenience in work operations.
3. To reduce costs for procuring new work equipment for employees.

General Criteria

1. Devices brought by employees must have specifications equal to or better than those specified by IT Support in order to effectively support the objectives of the department.

2. Devices brought by employees must have legally licensed Operating Systems (OS) and software installed. Employees are solely responsible for all software licensing fees for computer programs installed on their devices.
3. Devices brought by employees must undergo security software inspection by the IT Support department at least once a year. If it is found that any information technology software has been illegally copied, the employee must immediately purchase and install legally licensed software. Employees are required to strictly comply with the company's information technology policies.

11. Artificial Intelligence (AI) Policy

This Artificial Intelligence Policy (AI Policy) of MFEC Public Company Limited (MFEC) is established to define a safe usage framework for Artificial Intelligence (AI) technology in alignment with the Information Security Management System Policy (ISMS Policy), ISO/IEC 27001:2022 standard, and the guidelines of the IT Governance Committee.

Objectives

To define a safe AI usage framework in alignment with:

1. The latest Information Security Policy
2. ISO/IEC 27001:2022 standard
3. IT Governance Committee 2025 guidelines

Guidelines

1. AI tools may be used only when handling Public-level information.
2. In cases where AI tools are used with Internal Use or higher-level information, prior approval from the supervisor is required on a case-by-case basis.
3. Do not share any chats or messages publicly through AI services such as Gemini or ChatGPT.
4. Report any incidents in accordance with the incident handling procedures of the ISMS Policy.
5. Software Development Policy
6. Objectives
7. Establish development standards: Create a structured and high-quality framework for software development.
8. Reduce risks and prevent errors: Focus on minimizing risks and preventing mistakes in the development process.
9. Promote collaboration: Encourage effective collaboration and communication between teams.

10. Comply with applicable laws and relevant standards: Ensure that the development process meets all applicable legal and relevant standard requirements.

Guidelines

1. Policy compliance: All development projects must comply with the policies and guidelines set forth in this document.
2. Use of tools and technologies: Development must use tools and technologies approved by the ISMR or the Head of IT Support.
3. Communication and reporting: Communication and progress reporting must be carried out regularly, providing clear and accurate information.

Security

Objective

To ensure the security of data and systems from cyber threats.

Guidelines

1. Configure firewalls and intrusion prevention systems to prevent unauthorized access.
2. Regularly update software and operating systems to patch vulnerabilities that could be exploited in attacks.
3. Provide employee training on cybersecurity awareness and malware handling.

MFEC

Security
Our Responsibility