MFEC

Information Security Policy

Version 1.0

Information Security Policy

Information Security Maintenance Policy As MFEC Public Company Limited (MFEC) has implemented information systems for operations and services, serving both internal and external users, it is essential to ensure the appropriate, efficient, and secure use of information and information technology systems. This is to facilitate continuous operations, prevent issues arising from inappropriate use, and protect against threats. These measures help mitigate risks that may impact operations, assets, and personnel.

The maintenance of information security involves preserving the confidentiality, integrity, and availability of information and information technology systems at MFEC. This encompasses not disclosing information or systems to unauthorized individuals (confidentiality), ensuring the accuracy and completeness of information (integrity), and providing authorized individuals with access and functionality as needed (availability).

Therefore, MFEC has established a comprehensive information security maintenance policy comprising policies, guidelines, standards, and procedures. These are designed to align with legal requirements, standards, and international best practices for information security.

For detailed information and the structure of the Information Security Maintenance Policy document, please refer to the attached document. The components and structure of the Information Security Maintenance Policy are outlined for easy reference and understanding.

Objectives of Information Security

1. To establish and announce policies, guidelines, requirements, and procedures for executives, administrators, system administrators, and external individuals working with MFEC. This ensures that they are aware of the importance of maintaining information security and follow appropriate practices.
2. To instill confidence in the information security of MFEC, ensuring that access is restricted to authorized individuals (Confidentiality), information is accurate and complete (Integrity), and systems are readily available for use (Availability).
3. To develop systematic processes for managing information security and consistently

improve them.

4. To comply with regulations, directives, contracts, and laws related to information technology security.

These objectives collectively aim to create a comprehensive and robust framework for information security within MFEC, fostering a culture of awareness, compliance, and continuous improvement.

Guidelines

Practices in Information Security Technology (refer to Document MFEC-ISMS-PO-002)

1. Conduct studies, develop and create detailed operational procedures, organizational context, user requirements, and define the scope of information security operations to serve as guidelines for implementation.
2. Establish a standardized framework for information security operations as a clear model for operations.
3. Involve senior management in formulating information security policies and defining the roles and responsibilities of personnel involved in information security operations.
4. Define the objectives of information security and consider risk assessments to develop an annual information security plan.
5. Allocate resources to support knowledge development, awareness, and communication among personnel involved in information security. Also, document processes to achieve the objectives of information security.
6. Monitor projects and processes in information security to ensure compliance with the established plan.
7. Evaluate the effectiveness of information security operations in various dimensions, including policies, employee understanding, operational processes, relevant laws, and information technology.
8. Monitor compliance with practices from independent information security units to ensure transparency and efficiency in operations.
9. Compile reports on operational results for management awareness and decision-making to improve the efficiency and effectiveness of information security operations.

1. Access Control Sub-Policy

MFEC Public Company Limited (MFEC) has controls in place for data and information system usage, aiming to define measures to control unauthorized access to information and information systems. These controls are intended to prevent physical intrusion, network-based attacks, and attacks from programs that could cause damage to data or disrupt systems. Additionally, the controls allow for the verification and tracking of individuals accessing the organization's information or information systems. The principles guiding these controls are as follows:

1. Confidentiality: Only authorized personnel should have access to confidential information, and access control should ensure that sensitive data is not disclosed to unauthorized individuals.
2. Integrity: Ensure the accuracy and completeness of data by controlling errors and preventing unauthorized modification, deletion, or changes by unauthorized personnel.
3. Availability: Authorized individuals should have the ability to access and use data at agreed-upon times. Those responsible for access control must prevent system downtime, ensure continuous operation, and protect against actions that could lead to system disruptions.

Objectives of Information Access Control

1. To establish guidelines, requirements, and operational procedures for executives, administrators, system administrators, and external individuals working with MFEC. This ensures awareness of the importance of data and information system usage and access.
2. To instill confidence in the information security of MFEC, ensure that access is limited to authorized personnel with confidentiality, integrity, and availability.
3. To enable retrospective examination of user access to various information systems.

Guidelines:

1. Establish operational guidelines and procedures for data usage and information system access. Ensure that these are in line with laws, principles, and international standards for maintaining information security.

2. Ensure that information, information technology systems, information technology equipment, locations, and environments related to information, as well as the development and maintenance of information systems, are appropriately and sufficiently secured. Clearly define control procedures for usage and access in accordance with operational requirements.
3. Develop practical guidelines for software development that control access and permissions within the system, including operating systems, and ensure appropriate and secure data usage within users' computers.
4. Implement operational guidelines for controlling access to computers and information devices.
5. Establish operational guidelines for controlling access to server rooms or data centers on the Internet, including information devices accessible only by authorized personnel.
6. Ensure that users are knowledgeable about policies, regulations, operational guidelines, and procedures related to data and information system usage. Users must strictly adhere to and follow these guidelines.

Scope of the Information Access Control Sub-Policy:

The scope of the Information Access Control Sub-policy refers to the access of information, information systems, information technology systems, information networks, network infrastructure, and information technology equipment. Information encompasses both electronic and non-electronic formats.

2. Data Classification Sub-Policy:

MFEC Public Company Limited (MFEC) implements a data classification framework to ensure that information users and data owners are aware of appropriate practices. This classification system aids in aligning information management practices with the principles of maintaining confidentiality, integrity, and availability. It guides the organization in appropriately handling information in accordance with established principles for the proper management of information.

Objectives of Information Access Control

1. To establish guidelines, requirements, and procedures for executives, staff, system administrators, and external individuals working with MFEC to be aware of the importance of managing and maintaining information data, from creation to use and until it is no longer in use.
2. To instill confidence in the information security of MFEC, ensure that access is granted only to authorized individuals (confidentiality), that the information is complete and intact (integrity), and that it is available for use as needed (availability).
3. To raise awareness among employees regarding the security of information data.

Guidelines:

1. Establish written guidelines and procedures for the usage and access of information and information systems, ensuring compliance with laws, principles, and international standards for maintaining information security.
2. Provide users with knowledge of policies, regulations, guidelines, rules, and procedures related to the use of information and information systems. Users must adhere to and strictly follow these guidelines.

Scope of the Sub-Policy on Data Classification.

The scope of the sub-policy on data classification refers to establishing guidelines for the handling of information types, starting from creation or acquisition, usage, copying, and distribution, until the cessation or destruction. It covers information in electronic and non-electronic formats.

3. Operation Security Sub-Policy

MFEC Public Company Limited (MFEC) has established this policy to ensure that routine operations are adequate, performed accurately, and secure according to the standards of maintaining confidentiality, integrity, and availability.

Objectives of Operation Security

1. To establish guidelines, requirements, and procedures for executives, system

administrators, and external personnel conducting operations for MFEC to be aware of essential activities in information operations.

2. To instill confidence in the assurance of information and information system operations in terms of prevention and recovery in the event of issues with information or information system functionality.
3. To provide executives with appropriate reports for information security operations.

Guidelines

1. Develop operational guidelines and procedures for accessing information and information systems in writing, aligning with legal principles and international standards for information security.
2. Ensure that users are informed about policies, regulations, operational guidelines, rules, and procedures related to the use of information and information systems. Users must adhere to and strictly follow these guidelines.

Scope of the Sub-Policy on Operation Security

The scope of the sub-policy on operational security refers to establishing operational guidelines necessary to create 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 security in both internal and external communications within the organization, following the standards of maintaining confidentiality, integrity, and availability.

Objectives of Communication Security

1. To establish guidelines, requirements, and procedures for executives, system administrators, and external personnel conducting operations for MFEC to be aware of essential activities in information communication.
2. To instill confidence in the assurance of information exchange operations in terms of

prevention.

3. To ensure that information system users have confidence in communicating information within and outside the organization.

Guidelines

1. Develop operational guidelines and procedures for accessing information and information systems in writing, aligning with legal principles and international standards for information security.
2. Ensure that users are informed about policies, regulations, operational guidelines, rules, and procedures related to the use of information and information systems. Users must adhere to and strictly follow these guidelines.

Scope of the Sub-Policy on Communication Security

The scope of the sub-policy on communication security refers to establishing operational guidelines necessary to create confidence in the use of information and information technology systems.

5. Continuity Management of Information Technology Systems Sub-Policy

As MFEC Public Company Limited (MFEC) has established guidelines for prevention and preparedness in crisis situations, ensuring continuous operations is crucial for MFEC to fulfill its mission seamlessly. Therefore, a sub-policy on the continuous management of information technology systems has been instituted to respond to and mitigate the impact on critical operational processes that depend on information technology systems. This is to ensure that information technology systems can operate continuously at an agreed-upon level, involving stakeholders in the process.

Objectives of IT Systems Continuity Management

1. To analyze, plan, prepare, review, and rehearse essential processes as necessary.
2. To enable the continuous operation of information systems at an agreed-upon level during emergencies.
3. To ensure mutual understanding and awareness of roles and responsibilities in emergency situations among stakeholders.

Guidelines

IT systems continuity management involves preparing backup processes or systems that can substitute for the main system during emergencies. This aligns with agreed-upon conditions, considering Business Impact Analysis (BIA), Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). The policy includes:

1. Establishing a task force for IT systems continuity management aligned with MFEC's operational guidelines. This includes planning, implementation, drills, and continuous improvement.
2. Collaborating with the risk management and internal control committees to oversee the development of the IT systems continuity management system's overall operations.
3. Collaborating with the security department to coordinate the interdependence of information systems within the emergency response and crisis management framework.
4. Developing and maintaining the IT systems continuity management system is within the scope of responsibility. This includes planning, implementation, drills, and continuous improvement. It also involves assigning responsibilities for creating plans to safeguard critical infrastructure for IT system operations and reporting operational results periodically to the risk management and internal control committees.
5. Ensuring that executives, officers, employees, and related personnel have knowledge and awareness of their involvement in IT systems continuity management, contributing to the effective performance of their duties.
6. Ensuring that executives, officers, employees, and related personnel receive knowledge and awareness to actively participate in IT systems continuity management, contributing to the effective performance of their duties.

Scope of the IT Systems Continuity Management Sub-policy

The scope includes processes, service provision, workplace practices, and information services supporting critical operations within the policy. It can be considered based on significant factors involving processes dependent on information systems, the criticality of

information technology system recovery, downtime tolerances, contractual agreement timelines, and essential project timelines.

The scope of the policy sub-area on the continuous management of information technology systems.

The scope of processes, service delivery, the workplace, and the continuous system requirements of information technology, as well as information services that support critical processes within the scope of this policy, can be considered based on significant factors. These include processes that rely on information systems.

- Key Information-Dependent Processes: Critical processes that depend on information systems include those within project management, financial and accounting systems, payment processing, document storage, electronic document and correspondence systems, and the main website of the office.
- The importance information technology system recovery
- Maximum Tolerable Period of Disruption (MTPD) and the target time for recovery (RTO).
- Requirements regarding the timeframe in the processes of making contracts, financial disbursements, and accounting, as well as various project-related activities.
- Requirements of the Information Technology department, responsible for providing fundamental information services to the office, including being a service provider for information systems, computers, and network equipment.
- Key risks in the main workplace that may impact critical system services include the operation room, network servers, and network equipment in the office. Key risks include relying on technology services from specific service providers.

6. Information Security Risk Management Sub-Policy

Risks can arise from various factors in various forms, and the use of information technology as a tool in operations can pose risks to the organization. The significant risks include access risk to information and computer systems, management risk of computer systems, and inadequate computer personnel infrastructure risk. These risks can have impacts on the organization and its stakeholders. Therefore, a regular risk assessment is necessary to

appropriately manage risks, ensuring the security and continuity of information systems.

Purposes:

1. Conduct inspections and assess the risks of information systems or security situations that may be unforeseen or unpredictable.
2. To consider preventive measures and reduce the level of risks that may occur in information systems.
3. To serve as a guideline for actions in the event of risks that pose a threat to information systems.
4. To certify that the organization's information storage complies with security and personal privacy policies and laws.
5. To align with MFEC's risk management guidelines.

7. Supplier Management Sub-Policy

MFEC Public Company Limited (MFEC) has established this policy to instill confidence in managing resources from both internal and external service providers. This encompasses risk analysis and risk management with service providers, ensuring the integrity and security of information and information technology systems.

Objectives of Secure Operations:

1. To define guidelines, requirements, and procedures for executives, officers, system administrators, and external individuals working with MFEC and to be informed of essential activities for providing services from both internal and external service providers.
2. To instill confidence in supporting operations and addressing issues related to information technology systems from external service providers who act as vendors or manufacturers.
3. To foster readiness in reducing risks that may arise from both internal and external service providers.

Guidelines:

1. Evaluate risks related to both internal and external service providers to identify measures for addressing risk issues.
2. Establish guidelines and operational procedures for managing service providers as a written policy, in accordance with laws, principles, and international standards for maintaining information security.
3. Inform stakeholders about the guidelines and operational procedures for managing service providers and ensure that operations are conducted accurately and appropriately.
4. Conduct reviews of the practices of stakeholders to instill confidence that operations are carried out according to the designed directions.

Scope of the Sub-Policy on Supplier Management:

The scope of the sub-policy on supplier management refers to managing both internal and external service providers through agreements and contracts signed by representatives of both contracting parties.

8. System Acquisition and Development Management Sub-Policy

MFEC Public Company Limited (MFEC) has established this policy to ensure confidence in system acquisition and development for security and smooth operation without adversely affecting the business.

Objectives of Secure Operations:

1. To establish guidelines, requirements, and operational procedures for executives, staff, system administrators, and external individuals working with MFEC to understand the necessary activities for system acquisition and development.
2. To instill confidence in the acquired or developed systems that they can operate efficiently.
3. To reduce the number of complaints and disruptions in inefficient system operations.

Guidelines:

1. Establish operational guidelines and procedures for managing system acquisition and development that are clearly defined, aligning with laws, principles, and international standards for maintaining information security.
2. Inform stakeholders of the operational guidelines and procedures for managing system acquisition and development.
3. Implement policies and guidelines to build confidence in efficiently delivering and accepting systems.

Scope of the Sub-Policy on System Acquisition and Development Management:

The scope of this sub-policy covers the care of existing information technology systems at the main and backup data centers, as well as processes related to stakeholders involved in system acquisition and development. This includes individuals who have interests, both positive and negative, in system acquisition and development.

9. Personnel Resource Management Related to the Information Security Sub-Policy

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

Objectives of Secure Operations:

1. Define operational guidelines, requirements, and procedures for managers, staff, system administrators, and external individuals working with MFEC to understand necessary activities related to personnel resource management.
2. Acquire knowledgeable and capable personnel and develop existing personnel to align with the company's operational direction.
3. Reduce the risk of information leakage resulting from company personnel.

Guidelines:

1. Establish clear operational guidelines and procedures for managing personnel resources, aligning with laws, principles, and international standards for information

security.

2. Inform stakeholders of the operational guidelines and procedures for managing personnel resources.
3. Implement policies and guidelines to instill confidence in the existing personnel's ability to work in response to business requirements.

Scope of the Sub-Policy on Personnel Resource Management:

This sub-policy covers both internal organizational personnel and external stakeholders, such as outsourced or third-party entities, who must adhere to personnel resource measures.

MFEC

Security
Our Responsibility