บริษัท เอ็ม บี เค จำกัด (มหาชน)
MBK Public Company Limited
444 ชั้น 8 อาคาร เอ็ม บี เค เซ็นเตอร์ ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 ทะเบียนเลขที่ 0107537001102
444 8th Fl., MBK Center, Phayathai Rd., Wangmai, Pathumwan, Bangkok 10330 Thailand Registration No. 0107537001102
โทรศัพท์ (Telephone): +66 (0) 2853 9000 โทรสาร (Fascimile): +66 (0) 2853 7000 www.mbkgroup.co.th

Information Security Policy of MBK GROUP

As the MBK GROUP (the "Organization") has chronically used information technology systems to operate its business, it has a large number of important information considered as its information asset. The management team of the MBK GROUP has realized the importance of this matter and has established a information security policy to ensure that the implementation of the MBK GROUP's information systems is safe and compliance with current laws, rules, regulations, procedures on cybersecurity. The details are as follows:

1. Objectives:

To ensure the security and reliability of the information technology management of the MBK GROUP, that meets the international standards and be in compliance with regulations, rules, procedures, and laws on information security, as well as having a framework for an information security management. Therefore, 3 main objectives and goals in security management are established as follows:

1.1 To protect and maintain the security of important information of the MBK GROUP as well as its employees and customers.

1.2 To set a standard for operations and comply with rules, procedures, regulations, and laws on information security as stipulated.

1.3 To increase the efficiency of information technology systems so that they are protected against internal and external threats.

2. Definition

None

3. Scope

This procedure shall be used as a guideline for employees of the MBK GROUP.

4. Procedures or Guidelines

4.1 Information Security Policy

4.1.1 Risk Assessment

The MBK GROUP shall provide the Information Technology Risk Management, which covers Risk Identification, Risk Assessment and Risk Control at an acceptable level, as well as providing the personnel with responsible for managing information technology risks appropriately.

4.1.2 Information Technology Resource Management

The MBK GROUP shall provide the Information Technology Resource Management that aligns with its strategic plans and is adequate for information technology operations, as well as providing the key risk management in the event that sufficient resources cannot be allocated to information technology operations.

4.1.3 Information Technology Access Control

The MBK GROUP shall establish the appropriate access control for its information systems based on the category of data, data classification or priority to prevent unauthorized access from intruders and unwanted programs that may damage its corporate data.

4.1.4 Domain Registration for Business Operations

Companies under the MBK GROUP that use emails to communicate on any matters related to business operations of the MBK GROUP shall proceed as follows:

4.1.4.1 Provide the domain name registration for emails in the format of .co.th or .com, which state the company name or its business.

4.1.4.2 Determine administrators of the domain name who are responsible for checking the accuracy and security, renewal, as well as making changes to information and coordinating with relevant agencies.

4.1.4.3 Collects the document for details of domain name registration and provide an opportunity for authorized persons to inquire at any time upon request

4.1.5 Establish the backup system and contingency plan in case of emergencies.

The MBK GROUP shall provide the appropriate backup system in place and ready for use by selecting key information systems, as well as preparing a contingency plan in case of emergencies when electronic means cannot be used to ensure that information can be obtained normally and continuously. The personnel shall be assigned to be responsible for information systems, backup systems, and preparation of a contingency plan in case of emergencies when electronic means cannot be used.The contingency plan shall be tested and adjusted regularly for consistency with the actual implementation.

4.1.6 Preparation of Information Security Procedures

The MBK GROUP shall provide the procedures in place to maintain information security, which conform to the information security policy as stipulated and announce such procedures to relevant parties. The information security procedures shall cover the following important contents at the least:

4.1.6.1 Organization of Information Security

4.1.6.2 Human Resource Security

4.1.6.3 Asset Management

4.1.6.4 Access Control

4.1.6.5 Cryptography

4.1.6.6 Physical and Environmental Security

4.1.6.7 Operations Security

4.1.6.8 Communications Security

4.1.6.9 System Acquisition, Development and Maintenance

4.1.6.10 Supplier Relationships

4.1.6.11 Information Security Incident Management

4.1.6.12 Information Security Aspects of Business Continuity Management

4.1.6.13 Compliance

4.1.6.14 The MBK GROUP shall review the information security policy and procedures as well as other relevant procedures at least once a year to ensure that they are up-to-date.

4.1.7 The improvement and/or creation of a website or a web application shall comply with the Personal Data Protection Act as follows:

4.1.7.1 Has a Cookie Consent system in place, which requests consent to store cookie files and various information from website users.

4.1.7.2 Has a Cookie Policy displayed on the website to demonstrate the purpose of Cookies on that website.

4.1.7.3 Has a Privacy Policy displayed on the website to inform the data subjects of details and purposes of the storage and processing of personal data.

4.1.7.4 Has a Privacy Notice according to Section 23 of the Personal Data Protection Act B.E. 2562to inform the data subjects of the conditions regarding the processing of personal data as specified by law.

5. Exception

None

6. Penalty

Refer to the Company's work regulations.