Information Technology Security Policy

1. Objective

This Information and Technology Security Policy intends to maintain the security of information, that consist of confidentiality, integrity, and availability of the information technology system and the network and computers of Dhipaya Group Holdings Public Company Limited (the "**Company**"), ensuring that they are secure, able to continuously and effectively support the operations of the Company , are in compliance with the relevant laws relating to the information system, and prevent any potential threats that might damage the Company.

2. Enforcement

This Policy applies to Dhipaya Group Holdings Public Company Limited, its subsidiaries, including the executives, employees, and its suppliers that are within the scope of the information security management system.

3. Definitions

The Company means Dhipaya Group Holdings Public Company Limited.

Employees means the personnel of the Company.

Third-party service provider means a juristic person or its agent who works for the Company and is hired, in accordance with the Company's regulations, for an operation period that has been agreed in a relevant contract.

Information assets means all types of databases, data files, software, development tools, computer equipment, network equipment, communication equipment, external storage devices, and peripherals.

Information system means the system that links hardware, software, personnel, procedures, and data for the preparation of information for the Company.

Information means any data that has been changed, processed, or that has been analyzed and summarized by various methods, and is collected for further use as is required. Processing refers to the processing of data collected from various sources via various procedures and converting it to a desirable format to be used in the business of the Company.

4. IT Governance

The objective of IT Governance is to ensure that the Company will be able to achieve the specified goals by applying information technology as a supporting tool and managing any potential risks that may arise. In order to apply information technology efficiently, a sound information technology management must link the information technology management process with resources and data efficiently, in order to support the Company's policies, strategies, and goals, and an appropriate risk management system. In addition, the IT Governance activities must be reported and monitored to ensure that the technology applied by the Company can support the strategies, achieve business goals, and appropriately enhance its competitiveness.

5. Policy

The Company, therefore, issues the Information and Technology Security Policy as follows:

5.1. IT Security

5.1.1. The Company issues the Information and Technology Security Policy in writing and communicates this Policy to ensure understanding and correct compliance. The Information and Technology Security Policy is reviewed at least once a year or at every change that could affect the security of the technology information of the Company.

5.2. IT Risk Management

5.2.1 IT risk management: the Company ensures that the procedures or guidelines on information technology are able to mitigate risks or manage the existing risks relating to information technology, whether they be physical or environmental risks.

5.2.2 Risks associated with unauthorized access of the information system, i.e., servers, network equipment and other equipment, in which access must be controlled and its use must be restricted to authorized persons only.

5.2.3 Risks associated with using computer programs on the computers of the Company: to prevent any use or the installation of unsafe or malicious software, for example, downloading external programs that may contain malware or computer viruses, or any loopholes in connection to the external networks, attacking the computer that any person is using or other computers on the same network.

5.2.4 Risks associated with using the Company's computer network system: the internal network and the Internet system must be inspected and monitored. A system is in place to prevent any external access or any threats to the servers and clients, for example, a system for prevention of the entry and exit of the system

via the Internet, by the installation of antivirus software, and the screening incoming and outgoing emails, etc.

5.2.5 Risks associated with persons: the right to use and access the system, computers, network equipment, and data must be defined according to a person's rights, so as to prevent any editing or the changing of any data due to the inappropriate management of rights that could allow a wider access to data that is beyond one's own duty, and may damage such data and information.

5.2.6 Risks associated with perils and emergencies due to disasters, including other situations, for example, power outages, protests, etc.

5.2.7 Management-related risks arising from the inconsistency of the existing policies and the potential risks.

5.3 Asset Management

5.3.1 Information assets must be registered. Data owners must jointly prepare the register of these information assets. Labels must be issued and placed on information asset equipment.

5.3.2 The Company must classify and prioritize documents in accordance with the classification guidelines, in order to appropriately protect information assets. Documents or printed or duplicated materials, whether classified as a whole or in part, shall be considered to be in the same classification as the originals.

5.3.3 Information assets must be properly used. Rules, regulations, or criteria must be issued in writing to prevent any damage to information assets.

5.4 Human Resource Security

5.4.1 The employees and the suppliers must recognize their responsibilities, perform their duties in relation to their information security, and protect the interest of the Company, and this forms an integral part of the end of employment or any change in employment.

5.4.2 The duties and responsibilities on information security must be issued in writing for users and all external organizations that have been engaged, and preventive measures for the security of r the information of the Company must be issued.

5.4.3 In all cases, the qualifications of job applicants must be thoroughly checked, for example, checking recommendation letters, work experience, educational background, or training, etc. For all new employees the importance of basic security must be given,

impressed and cultivated. Employees in the units or departments that can access sensitive information of the Company must sign confidentiality agreements.

5.4.4 All users employed by the Company, must comply with the security measures in line with the policy of the Company.

5.4.5 The users must be trained on the importance and procedures for security of the information technology and information. Records of training must be signed and kept in the personnel record files. The employees must also be informed of any change to any information and technology.

5.4.6 Any person violating the policy, rules, and procedures of the Company will be subject to disciplinary action. Any person violating the law, will be subject to punishment by law and in accordance with the Work Rules.

5.4.7 In the case of any appointment, transfer, dismissal, or change of any position, the Human Resources and Administration Department must inform the employees and the employees must comply with the conditions of the employment contract until the end of their employment. An employee, whose employment ends for any reason, must return all assets relating to the information system, for example, keys, employee identification card, peripherals, manuals, and documents, to the supervisor before the last day of employment, and the Information Technology Department must revoke the right for such person to use the information system.

5.5 Physical and Environmental Security

5.5.1 All employees and suppliers must comply with the guidelines on physical and environmental security specified by the Company to prevent any unauthorized physical access, damage, or interference of the operation of information data processing equipment and the information operating system of the Company, as well as to prevent any interruption to the operations of the Company.

5.5.2 Physical and environmental security must be established in the offices, room offices, and other properties. Measures must be established to prevent threats, for example, fire, flood, earthquake, unrest. In addition, any operation in the secured area must be appropriately protected.

5.5.3 Deliveries of goods by third parties must be made in a specific area, in order to prevent unauthorized access to the information assets of the Company.

5.5.4 The employees have the duty to protect office equipment in order to minimize any risk associated with physical threat or peril, including risks associated with any unauthorized access to the equipment.

5.5.5 The information assets must be kept in a safe place and the operating area of the information system must be appropriately separated. The computer center must be in a separate room from the general office area. Access and egress to the secured area must be controlled and only those persons, who are authorized in writing, are allowed to enter.

5.5.6 A power backup system must be provided for important equipment to ensure a continuous operation, and the power backup system must be inspected on a regular basis to minimize any potential damage.

5.5.7 Cable routing must be protected against unauthorized access, and signs and labels must be properly attached to identify the origin and the destination.

5.5.8 The computer system, the network system, and the servers must be properly maintained on a regular basis, or at the periods as specified by the manufacturer.

5.5.9 Protective measures must be in place for equipment that is installed outside the office, to protect it from any damage.

5.5.10 Any equipment with storage media must be checked to ensure that any important information has been deleted or saved before discard, in accordance with the procedures specified by the Information Technology Department.

5.5.11 Protocol for handling portable storage media must be issued.

5.5.12 Preventive measures must be issued for any unauthorized access to documents in the system .

5.5.13 Protocol for the handling and the storing of information must be issued, to prevent any unauthorized access.

5.6 Supplier Relationships

5.6.1 The employees and the suppliers must comply with the supplier security guideline specified by the Company to protect the assets of the Company as accessed by suppliers, and to maintain the security level and the service level as agreed in the service agreements of all suppliers.

5.6.2 Service agreements must be made in order to control the service of external organizations, for example, external organizations must

accept the Information Technology Security Policy and its scope and details, and the service level must be reviewed by the Legal Department, including all non-disclosure agreements, etc.

5.6.3 External organizations or other third parties that are allowed to access the information system of the Company must accept and comply with the Information Technology Security Policy.

5.6.4 The Company will assess potential risks associated with access to the information system or any impact upon the Company by external organizations or other third parties. If it is necessary to disclose any information, all external organizations or other third parties must sign non-disclosure agreements with the Company.

5.6.5 The services or agreements made with external organizations and third parties providing services to the Company must be reviewed on a regular basis as necessary, and the scopes of services must be revised; for example, in the case of any improvement of the information system, development of the information system, or the introduction of new technology.

5.7 Access Control

5.7.1 A procedure for registration for rights and access to the information and the information system of the Company as necessary, including the procedure for the cancellation of rights must be in place, for example, upon any resignation or change of position. In addition, a procedure for the management of user passwords must be in place, to ensure that the allocation of passwords to users is appropriate and related to all delegated tasks.

5.7.2 Users must be responsible for their user accounts and passwords to ensure that these are secure.

5.7.3 The employees must prevent any unauthorized persons from accessing office equipment that is unattended. For example, in the case of any unattended office equipment, the unit head or a security guard must be informed. In addition, the Company has a policy that important information assets, for example, documents or storage media, are never left in any unsecured place or in any place that can easily be seen.

5.7.4 A guideline on the use of network must be issued and this must state which service is allowed for the users and which service is not allowed for the users.

5.7.5 Any access to the information system or the information of the Company must be approved by the unit head and the head of the Information Technology Department, and is only allowed for an

area that is related to one's duty. Only authorized persons or those persons on a need-to-know basis are permitted access, and only after the consent of the data owners has been obtained.

5.7.6 All and every access to the information system and information of the Company requires authentication, whereby the right of such access must be reviewed at least once a year.

5.7.7 Any change to the information system, the network system, or any application must first be checked and permission granted by the data owner, and approved by the head of the Information Technology Department.

5.7.8 Measures must be issued to prevent any access to the port used for inspection and adjusting the system. These measures must cover the protection of physical access and access via the network.

5.7.9 A system or method for verifying the quality of passwords must be in place, to ensure that the users change their passwords after a specified period.

5.7.10 The use of the utility program must be limited and controlled in order to prevent any breach or avoidance of the security measures, for example, the utility program must be limited to only the authorized persons. Cutting-off times for using computers must be in place in order to increase the life span of computers, and the connection time of the information system that is of great importance must be limited.

5.7.11 All systems that are extremely important must be segregated in a separate area, and a policy, plan, and procedure must be defined for those users who are required to work outside the office.

5.7.12 Any access to any applications must be controlled and restricted, and only authorized or delegated persons, for example, the system administrators are allowed access. In addition, the use of proprietary software is allowed, but only for the number of acquired licenses.

5.7.13 All access to the network must be controlled, and the right of access to the network must be assigned to users. The route for connecting the computer system with the Internet must be specified by directing it through the security system of the Company. The network has been designed into separate zones, in order that threats will be effectively and systematically controlled and prevented.

5.7.14 The operating system must be controlled by specifying user rights and user authentication before entering the system. Any user who does not use the system continuously during a specified period

must be cut-off, in order to limit the period for linking with the information system (session time-out). For portable computers and portable communication equipment, the Company has a policy that its users only use portable communication equipment of the Company in accessing or storing data or information of the Company. In the case that it is necessary to use personal portable communication equipment to access or store data or any information of the Company, specific permission must be requested and the personal portable communication equipment that is used to access or store data and information of the Company must be portable communication equipment that has not been modified so as to violate security or infringe copyright, in accordance with the policy specified by the Information Technology Department.

5.7.15 The network systems must be divided according to the service zones, for example, zones in the Company and zones outside the Company, in order to systematically protect against any threats.

5.8 System Acquisition, Development and Maintenance

5.8.1 The employees and suppliers must strictly comply with the System Acquisition and Development Policy in order that the security of information becomes an important component of the system and also the life cycle of the system acquisition and development, including the needs of services via the public network.

5.8.2 System developers and owners must set requirements of the security of the system that has been procured or developed by assessing all risks and identifying the security requirements so as to minimize such risks.

5.8.3 In order to prevent any error of data and information, loss of data and information, or use of information for the wrong purpose, system developers must specify all steps to verify information that is imported into the information system during the processing, and information that is exported from the information system, to ensure that the relevant data and information is accurate and complete.

5.9 Cryptography

5.9.1 The use of cryptography must be controlled and must be enforced by the Company. Keys for coding or decoding information must be properly applied using the standard cryptography techniques of the Company.

5.10 Information Security Incident Management

5.10.1 All users must report any security incident of the Company, for example, any possible weakness, to the supervisor or the Information Technology Department immediately upon the detection or suspicion of any irregularity. Duties and responsibilities to respond to security incidents are delegated, security incidents are recorded, and the type, magnitude, and expenses of security incidents are analyzed and considered.

5.10.2 Evidence must be collected in accordance with the relevant rules or regulations for use in court proceedings or other relevant proceedings.

5.11 Communications Security

5.11.1 The employees and suppliers must comply with the communications security guidelines specified by the Company to protect the information in both the network and the data processing equipment, to ensure the security of the information transferred within the Company or the information that is transferred to external organizations.

5.11.2 Operation manuals must be issued, for example, a system recovery procedure, a system maintenance procedure. In the case of any change of procedures or responsible persons, all manuals must be revised, and they must also be reviewed at least once a year. In addition, any change, improvement or modification to the computer system, the network system, servers, and hardware and software must be controlled.

5.11.3 The duties and responsibilities of system administrators must be segregated, in order to minimize any chance of unauthorized change or modification.

5.11.4 The development system and the testing system must be segregated from the actual operation system to prevent any access to data or change of the actual operation system by unauthorized persons, and the operation condition must be monitored and the capability of information resources must be analyzed on a regular basis and at least once a year.

5.11.5 In order to accept any new system, the acceptance criteria must be established, and the new system must be tested before inspection and acceptance in writing.

5.12 Information Security Aspects of Business Continuity Management

5.12.1 The employees and suppliers who are within the scope of the information security management system of the Company must comply with the continuity management guidelines of the information system, so that the information system of the Company is able to provide service continuously, and to enable the availability of the data processing equipment of the Company.

5.12.2 A business continuity management process must be prioritized; incidents that might or will cause business interruption must be identified; the likelihood and potential impact must be considered, and a business continuity management plan must be prepared for all important operating systems.

5.12.3 All business continuity management plans must be tested at least once a year, to ensure that in the case of any emergency, the business continuity management plans are able to operate in a real situation.

5.12.4 A framework for the business continuity plans must be defined, so that these plans are consistent and all the requirements of information security technology are covered.

5.12.5 The information system must be backed up in order to be able to provide continuous and stable services. The information system and the backup system must be appropriate and available. The system administrators have the duty and responsibility for the backing up of all data. In addition, a contingency plan in the case of any emergency or operational disruption must be prepared, and must also be reviewed at least once a year, in order to ensure the availability of the information system. The business continuity management plan must be reviewed and revised whenever necessary.

5.13 Operations Security

5.13.1 The Company and the Information Technology Department must use software that has a management protocol for the prevention of malicious software. Every employee must cooperate and comply with the policy and must refrain from the installation of software without receiving permission from the system administrators or any person who is delegated by the system administrator.

5.13.2 The employees and suppliers must comply with the operational security guidelines to ensure that the operation of the information data processing equipment, and the information operating system of the Company is accurate and secure: that any malicious software

is protected against, and loss of data is prevented. This is for the information system to record incidents, present evidence, ensure that the operation is properly functioning, and technical loopholes are prevented, in order to minimize impact on the evaluation activities of the service system.

5.14 Compliance

5.14.1 The employees and suppliers must comply with the relevant laws, standards, and regulations, and refrain from violating any obligation of the laws, regulations, rules, or engagement contracts related to information security, this is to ensure that the information security operation is in compliance with the organization policy and procedures:

- Information Technology Security Policy;
- Computer-related Crime Act B.E. 2550 (2007);
- Electronic Transactions Act B.E. 2544 (2001);
- Copyright Act B.E. 2537 (1994);
- Trademark Act B.E. 2534 (1991);
- Personal Data Protection Act B.E. 2562 (2019);
- and/or other relevant acts.

5.14.2 Any information that is created, stored or transmitted through the information system of the Company is considered an asset of the Company, with the exception of any information that is the property of customers or third-party software, or other materials that are under the protection of third-party patents or copyrights.

5.14.3 Data relating to legal requirements and guidelines, contract terms, and business terms, and personal data must be protected as specified by the relevant laws, guidelines, and agreements.

5.14.4 The information, the information system, the computer system, the network system, and the servers must be protected against any use for the wrong purpose, or any unauthorized use, and cryptography measures must be issued in line with legal requirements.

5.14.5 The Company can review and inspect every system of the Company without advance notice if it is considered necessary.

5.14.6 The security of the system must be tested by using software to identify loopholes and must be tested against any attack to identify all system bugs.

5.14.7 The requirements and the activities of the inspection of the information system must be issued, in order to minimize any impact on the business process; the software that is used in the system inspection must be protected again any use for wrong purposes by installing a tool for the separate inspection of the information system.

6. Punishment

In the case of any violation of this Policy, the Company will consider the imposition of disciplinary action in accordance with the Work Rules, and/or may take legal action.

7. Exclusion

If any employee or supplier, within the scope of the information security management system of the Company, is unable to comply with the Technology Information Security Policy or the guidelines specified by the Company, he or she must clarify his or her reasons and submit a letter requesting permission from the authorized person on a case-by-case basis, provided that such exclusion must be accompanied by the appropriate security measures.