10. Information Technology Policy

The Company has established a policy on information technology as it is an important factor that can help develop and promote the potential of business operations as well as increase the efficiency of employees in the organization. Therefore, the Company defines it a shared responsibility of every employee and at all levels to use information technology under the regulations of the law, the Company's orders, and standards for maximum benefit.

10.1 Objectives

(1) For employees of the Company to use the policy as a guideline and to use the Company's information technology effectively.

(2) To determine the utilization of the Company's information technology under the relevant laws, orders, and standards set by the Company.

10.2 Definitions

(1) Relevant laws mean computer systems and computer data per international standards, the Computer-Related Offenses Act, B.E. 2550

10.3 Regulations and Requirements

(1) Every employee and every level in the organization must abide by the Computer Crime Act B.E. 2550

(2) Confidentiality determines the type and order of information to prevent misuse of information. Information Classification requires that the division of organization's security levels by taking into account the level of security risk. The impact on the value and damage that users may receive can be divided into 4 levels as follows:

(2.1) Public Information: information that is intended to be known to customers or third parties.

(2.2) Internal: information only for employees of the organization to use.

(2.3) Confidential: information only available to employees of the organization.

(2.4) Highly Restricted: information of the utmost importance. If it leaks, it can cause damage. For example, information about a new administration that has not yet been declared.

(3) Procurement and installation of computer systems determine how to procure and manage the organization's computer systems that can support the organization's business services swiftly, continuously, accurately, reliably, and efficiently. The computer system changes control so that the work system can support the business of the organization continuously and efficiently. If there is a change in business requirements, a request for a change is provided, the written request is documented, and an impact analysis is required for the relevant parties to document a comprehensive impact analysis. The change control must be approved by the authorized person of each department and quality control of the service of the computer system so that the information technology system can provide continuous and reliable business response services.

(4) Disaster Recovery Center (DRC) and Disaster Recovery Plan (DRP) require a backup computer center and backup information technology systems to support business operations with backups to maintain accuracy and availability. The Disaster Recovery Plan, which aligns with the business continuity management strategy, was formulated for business departments to continually transact and resolve issues that arise swiftly, even in the event of an emergency or any security incident.

(5) The IT Insourcing and IT Outsourcing were controlled for the information technology operations aspect to be in accordance with the criteria of information security organizations, which requires a backup by using the storage media and should provide an insourcing standard. The criteria for considering outsourcing must not conflict with the rules or regulations announced by government agencies and stipulate clear and documented guidelines for IT outsourcing risk management appropriately to the importance of the work system that is being outsourced and in accordance with the overall risk management policy to formulate various requirements and operational framework for efficient, secure, and maximum beneficial IT insourcing and IT outsourcing to the organization.

(6) Information services provide sources of information for each department to use for analysis, research, and reports for executives to make informed decisions. The designation of who has the information usage authority in the data source must be approved only by the entity to which the information belongs. The information provided to external agencies must be approved by the authorized person only. Before delivery, the information must be validated by the person to whom it belongs.

(7) All employees of the Company have duties and utilization practices as follows:

(7.1) Be responsible for preventing and ensuring that the Company's information systems in their possession or responsibility will not be accessed without permission from an unauthorized person and do not disclose business-critical information to irrelevant parties.

(7.2) Have the Company's information systems and communication equipment utilization discipline so that it does not harm the Company and others, such as using it as a tool to access information systems without permission to damage reputation and assets, disturb or disrupt the operation of information systems, intercept information, hack, forge computer information, and disseminate inappropriate images, text, or sounds, and not used for personal business or illegal activities.

(7.3) Must not infringe on the software copyright or intellectual property of others.

(7.4) Must encrypt information when sending business critical data over the Internet and not exchange business critical data with unprotected websites.

(7.5) If an employee requests for an associate worker who is an employee of the Company's contractor to access the Company's information system, the employee who requests permission must control the use of the associate worker and be responsible for any damage that occurs to the Company.

(7.6) The Company will investigate, search, monitor, interrogate, and control employees' information systems utilization if there is any suspicion that employees improperly and reasonably use them to protect the security of the Company's information systems.

(7.7) The Company controls computer center access and damage prevention to prevent unauthorized people from accessing, acknowledging, modifying, or causing damage to information and computer systems.

10.4 Penalties

If the Company finds that the employee has violated compliance with the Computer Crime Act B.E. 2550 or the Company's information technology policy and fair investigation results appear to be true. The employee will be considered for disciplinary action of the Company and/or legal penalties as appropriate.