Information Technology Security Policy
of
Dynasty Ceramic Public Company Limited and its subsidiaries

Principles and Reasons

Any action in information technology of Dynasty Ceramic Public Company Limited (the "Company") and its subsidiaries stable, safe and reliable. Also the company's data and information assets be properly maintain. Company is aware of importance in use of information technology in business management. Therefore this policy has been set to provide framework for good governance and managing enterprise information system to be in line with the principles of good corporate governance, as well as other related laws to suit Company's business operation.

Information Technology Security policy

1) Inspection and information technology risk assessment.
2) Information technology risk management.
3) Security aspect of information technology systems.

1. Inspection and Information Technology Risk Assessment

In order to be relevant with organizational strategic plan and achieve the goals set as follows:

1) Set criteria and factors for prioritizing information technology plans to be appropriate and relevant with strategic plans and business goals
2) Prepare and approve an IT budget that is relevant with the budget plan and organizational strategic plan.
3) Managing adequate human resources for work in information technology by provide continuously personnel skills development, including hiring outside IT personnel when necessary.
4) Manage risk in event of not being able to allocate sufficient resources to carry out IT operation, whether personnel or budgets exceeding as specified.
5) Determine a duties and responsibilities of personnel IT department in allocating and managing information technology resources.

2. Information Technology Risk Management

1) Determine information technology risk management in accordance with the organization policy and risk management.

2) Determine on maintaining information system security is a part of business continuity management. This is to keep information system always in ready to use condition.

3) Determine management of events that may affect security of information system by specifying management processes steps and those responsible. Including providing quick and timely reporting of situation through person or agency who responsible for receiving event notification so that events and weakness related to security of information system are properly effectively handle in appropriate time.

4) Determine the management of the company's assets by specifies and defines responsibilities for maintaining the security of information assets to ensure that important information assets are properly protect.

3. Security aspect of information technology systems

Determine security aspect of information technology system by considering size characteristic and complexity of business operation. Including rules related to make users and related persons aware of the importance for maintaining information system security with inform responsibilities and guidelines for controlling risks which determines company's operating guidelines as follows.

3.1 Classification of information assets

Access control and usability of company's information to be appropriate for type of data, order of priority or level of data confidentiality, including data accessibility level, access times and access channels. Provide intrusion detection system from intruders, including unwanted programs that may damage information technology equipment or affect confidential or important information.

3.2 Organize backup data system and Contingency plans

Organize an appropriate backup data system to be ready in use. By selecting important information system, including creating a contingency plan in case of an emergency where electronic method cannot be use. The information can be use continuously normal and regularly test the availability of backup data systems.

3.3 Data encryption

Determine data encryption measure and guidelines for selecting data encryption standard to be appropriate for the risk that may occur with monitor compliance with the policy consistently.

3.4 Personnel Administration and Supervision

3.4.1 User

1.Determine information asset protection measure when detect device idle time

Users are require to access their computer or information technology system by enter password and immediately log out of information system and computer when no longer need or when finish work.

2.Determine mobile device usage and operations from external networks

Set an appropriate measures to control security of portable communication devices by consider risk of connecting devices to company's computer network, including setting control measures for using devices outside company.

3.Set up software installation control on working system

Making procedures and measures to control software installation on actual service system to limit software installation by use and prevent unauthorized software installation on system. Define a list of standard software that is permitted to be install on company's computer and updated. Including communicating to user within the company to acknowledge and observe.

3.4.2 IT Outsourcing Control

Create regulations and conditions of operation for external service providers to protect information assets from inappropriate assessment and control submitting work in accordance with agreement. This is also include operator who has other external executive take over management of information technology work.

3.5 Computer network organization and information transmission

3.5.1 Information communication through computer network

Supervise a computer network management control to be secure and control the determination of security feature, service level, and management requirement for network service in agreement or contract for network services, both within company group or external. Including separating system as appropriate by considering the need to access system, impact and importance level of that information.

3.5.2 Information transmission control

-Shall control and supervise a regulation for exchange data between departments, both within company group or external departments in writing.

-Determine measure to control a transmission of electronic message such as E-Mail, which must be appropriately protected attempt to access, modify or disrupt a system from unauthorized person.
- Arrange workers and external agencies that work for the company make a confidentiality agreement or non-disclosure agreement of the company in writing.

3.6 Protection against threat to information system

-From malicious software, the company shall determine measure for detection, prevention and system recovery to protect assets from malicious software.

-From technical vulnerability, the company must control information system to be proven for technical vulnerabilities that may occur by organizing penetration testing, organizing system vulnerability assessment, organizing testing of procedures and processes for managing incidents that may affect the security of information system at least once a year.

3.7 Procurement, Development and Maintenance of information systems

The company has the provision of appropriate information systems, development and maintenance to reduce error in the specification of requirements, design, development and testing of newly developed or further system improvements.

Policy Review

The policy shall be reviewed at least once a year to keep it current.

Reporting

The company shall report on compliance with the policy, including regulations and requirement to the Board of Directors at least once a year or in the event of any urgent events that affect compliance with the policy.

Approved by the resolution of the Board of Directors meeting No. 4/2024 on August 6, 2024.

(Mr.Roongroj Saengsastra)
Chairman