Announced IT.001/2022

Information Security Management System Policy

Objective

1.1 In order to maintain the security of information, which consists of confidentiality of information to maintain the integrity of the data and the availability of the data.

1.2 To provide management direction and information security support in accordance with business needs and relevant laws and regulations such as information security control procedure for staff and external service provider.

Introduction

Information Security Management Policy is established in accordance with the TISAX (Trusted Information Security Assessment Exchange) to provide management direction in accordance with business needs and relevant laws and regulations which requires compliance from staff and external service providers. The policy shall communicate to related parties. This Information Security Management Policy has categorized as following.

Project Management Policy

Employees within the scope of the Information Security Management System must comply with the Project Management Policy for control customer and company confidential information during the project management implementing such as improvement of the information technology, database system or ERP project, the network system improvement project, or the new product development (Advance Product Quality Planning: APQP).

Human Resource Security Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Human Resource Security Policy. Their responsibilities are defined for information security responsibilities and aware of asset and confidential data protection as part of the employment and company beneficial.

Asset Management Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Asset Management Policy. The asset protection has been defined in their responsibilities according to the appropriate level of protection and prevention of unauthorized disclosure, alteration, transfer, deletion or destruction of data or information stored on the storage medium.

Access Control Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Access Control Policy to control access to information processing which is allow for authorized persons only and prevents unauthorized access to systems and services. Therefore, the users are responsible for the protection of authentication data and will not access to the external website in case that it is not related to the operation, or violation to the laws or Computer Crime Act.

Cryptography Control Policy

Employees, and external service providers within the scope of the security management system must comply with the Cryptography Control Policy to ensure the effective password setting and prevent exposed to other unauthorized persons. The data encryption is required to prevent confidentiality, and authenticity. If there is something suspicious, change the password immediately and do not use the same password to other system which is not related to their works, or change the password when entering the system for the first time. The password setting must be at least 8 characters with special characters to make it difficult to predict. The login information is protected and non-disclose to third party.

Physical and Environmental Security Policy

Employees, visitor and external service providers within the scope of the Information Security Management System of must comply with the Physical and Environmental Security Policy to prevent physical unauthorized access, damage and interference with work equipment and information systems including preventing interruptions to the operation.

Operations Security Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Operations Security Policy to operate and the secure the asset protection from malicious programs to prevent the data loss. The data protection against exploitation is implementing by vulnerabilities technique to reduce the impact on the IT service system.

Communications Security Policy

Employees, business partners, and external service providers within the scope of the Information Security Management System must comply with the Communications Security Policy to protect the data transfer in networks when transfer the information processing between internal staff or transfer with external parties.

System Acquisition, Development and Maintenance Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the System Acquisition, Development and Maintenance Policy to make information security a key component of a system development throughout the System

Development Life Cycle (SDLC). This policy has been developed to control the direction and steps to make the new system development for little defects as much as possible because the system analysis and testing before use.

Supplier Relationships Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Supplier Relationships Policy for security of services received from the service providers, and to provide assets protection which are accessed by external service providers. Finally, the service levels agreement and information security can be achieved as defined in the Service Level Agreement.

Information Security Incident Management Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Information Security Incident Management Policy in order to have a consistent and effective methods for incident reporting. This includes notifying the information security situation and vulnerabilities to related departments.

Information Security Aspects of Business Continuity Management Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the Information Security Aspects of Business Continuity Management Policy to prepare the operation in case of disaster or abnormal condition including compliance with legal requirements and customer or contract requirements. Therefore, the BCP structure is establish and defined mitigation for potential treats in the company.

End User Oriented Policy

Employees, and external service providers within the scope of the Information Security Management System must comply with the End User Oriented Policy access to documents and sensitive data, internally transferred information is secured or transferred to an external party. The rule for software installation, assess management control, and network connection for end users is maintain the security for remote operations and internal connection from PC and mobile devices.

Management Review and Improvement Policy

This Information Security Management Policy will be reviewed in case of organization structure or top management has been changed (reviewed within 45 days after change). However, if there is no such change, this Management Review and Improvement Policy. The related procedures will be reviewed annually by top management together with TISAX Committee in the management review meeting. There are some agendas to be review with the policy such as Information Security KPIs result monitoring, asset control list, result of risk analysis and control measures (risk treatment plans), changes that occur and control effectiveness, conformity assessment results, TISAX standards and legal compliance status, incidents reporting, summary of reviews of Information Security documents and forms, results of Certify Body assessments and follow-up, suggestions for improvement. The management review results will be the management decisions and necessary resources supporting to the TISAX compliance and improvement.

Punishment

If there is a clear and serious offense violation even for the first time, top management and human resources departments will consider disciplinary actions. This may include the legal action which is punishable by both imprisonment and fine.

Exclusion

In case that the employees and external service providers within the scope of the Information Security Management System cannot comply with this policy, they need to notify their manager and prepare the permit documentation with the equivalent information security control.

Therefore announced for your acknowledgment and generally practiced.

Announced on July 1, 2022

....

(Mr. Poollarp Jittrasawad)
ITD Information Technology Asst. VP

....

(Mr. Athasidh Ongkosit)
ITD Information Technology Sr. VP

....

(Mr. Pitharn Ongkosit)
President and Chief Executive Officer