[Translation]

Third Party Security Policy

1. Introduction

1.1. Objectives

- To maintain the security of data and information systems of the Company when collaborating or using services from Third-Party
- To ensure that services received from Third-Party are accurate, secure, compliant with agreements, and that Third-Party takes care and uses the Company's computer equipment and assets cautiously

1.2. Scope

This policy covers various operations related to Third-Party and customers of the Company, including contracting, agreement execution, access control to data and information systems, operational oversight, and service auditing received.

1.3. Definition

- Vendor refers to both sellers of goods and service providers
- Third-Party refers to vendors, customers and partners who need to access the data and information systems of the Company or use the Company's computer equipment or assets.

2. Policy

2.1. Working with Vendors

- When contracting vendors, a selection process must be undertaken, assessing their qualifications and capabilities according to the Company's guidelines. The level of importance of the data and information systems that vendors need to access should also be considered.
- Every Third-Party engaged in business with the Company must sign the following documents, as appropriate, before commencing operations:
  1. Contract and/or Service Level Agreement
  2. Non-Disclosure Agreement

All contractual documents must undergo appropriate legal review.

- Vendor hiring unit and the Information System Security Management team, or assigned personnel may consider adding additional terms or protective measures in the contract documents to maintain the security of the Company's data and information systems. This depends on the nature of the job being contracted and results of risk assessment.
- In the case of contracts related to data exchange between the Company and other parties, additional clauses should be considered in the contract, including:
    1. Clearly defining the method used for data exchange and the responsibilities of both parties. The selected method must be reviewed and approved by at least from the AVP level upwards of the Information System Security Management team or assigned personnel.
    2. Clearly specifying labeling methods and delivery channels for data.
    3. Identifying the technology used to protect the data, such as data encryption.
    4. Specifying the procedures to be followed in the event of a security breach during data exchange.
- In the case of contracts for vendor software development, additional topics should be considered in the contract, such as:
    1. Stating quality and security requirements in the developed program and source code.
    2. Specifying agreements on copyrights and intellectual property of the developed program.
    3. Outlining the vendor's responsibilities regarding the quality and accuracy assurance of the developed program.
    4. Specifying the Company's rights to access and verify the quality and accuracy of the developed program.

- Vendors must communicate details of Third-Party Code of Conduct and other relevant agreements to their personnel in order to work properly when using the Company's data and information systems.
- Vendors must notify the Company of the names of personnel who will be working for them before commencing work and inform the Company in advance of any changes in personnel.
- Personnel of the vendor must strictly adhere to the rules, policies, procedures, and work instructions of the Company.
- All types of information obtained by the vendor from the Company must be kept confidential and may only be used for Company operations.
- In cases where the vendor's service is provided outside the Company's premises, the Company reserves the right to inspect all areas where the Company's data is used, transmitted, or processed.
- Equipment or software used by the vendor in their operations for the Company must be adequately maintained for security. At the minimum, they must have reliable virus protection software installed, and their databases must be up-to-date. The Information System Security Management team or assigned personnel may consider having the vendor install additional security software or measures as deemed appropriate.
- In cases where the Company's equipment and software are installed at the vendor's premises, all equipment and software must be recorded. Access to the equipment and connection to the Company's network must be carried out by Company employees only and must be used solely to support Company operations. The Company reserves the right to consider contract termination in cases of misuse of Company equipment or software.
- Access to the Company's data and information systems by the vendor must be controlled.
- Clear time frames must be established for granting access to the Company's information systems to the vendor.

- Access to the Company's information systems by the vendor must be limited to authorized systems only.
- Services provided by the vendor that require connection to the Company's network, remote access, or communication channels for data transmission to the vendor's system, including other activities that may pose risks to the Company's information systems, must be assessed for risk and managed appropriately. Approval must be obtained from the management, at least from the AVP level upwards of the Information System Security Management team or assigned personnel, before proceeding. Topics to be considered should include, at a minimum:

    1. Security of the location and/or systems to be connected to the Company's network
    2. Security of the devices that need to be connected
    3. Methods for verifying identity before granting access to the system
    4. Security of channels and methods for data transmission
    5. Methods for controlling and monitoring access or data transmission
    6. Other requirements to enhance security, such as limiting connection times
    7. Authorized duration for connections or data transmission, and appropriate intervals for risk assessment and security checks

- Vendors and/or their personnel are prohibited from using company copyrighted documents or software for personal purposes or in any unauthorized manner, and from using documents or software that infringe on copyrights in the Company's premises.
- The Company reserves the right to inspect the work of vendors, including revoking access rights to data and information systems, when abnormalities or security breaches are detected without prior notice.
- Vendor accesses to systems must be recorded and regularly monitored.
- Vendors must report any abnormalities or security breaches to system administrators and designated contact personnel immediately upon discovery.

- Any actions by vendor's personnel that cause damage or violate agreements or contracts with the Company, must be full responsible by the vendor.
- Vendors hiring subcontractors must notify the Company each time and ensure subcontractors comply with the Third Party Code of Conduct and agreements made with the Company. Vendors are responsible for overseeing and holding subcontractors accountable for all work and actions.
- Employees who liaise with vendors or relevant parties must conduct thorough inspections of the completeness of the work delivered by the vendor and ensure thorough testing to ensure that operations can indeed be carried out effectively.
- Employees who liaise with vendors or relevant parties must ensure that the work delivered are adhere to the terms outlined in the contract or SLA (Service Level Agreement) before accepting the work.
- Upon the termination of a work contract, changes to the contract, contract cancellations, or changes in personnel working for the vendor, the coordinating employees, system administrators, or assigned employees must ensure the return of all company assets and appropriately revoke access rights to systems.
- Any changes made by the vendor that may impact service provision as per the agreement or contract with the Company must be communicated to the Company at least 30 days in advance in written form, allowing the Company to assess, analyze the impact, evaluate potential risks, and find appropriate solutions to manage and control the risks.

2.2. Working with Customers and Partners

- Access to data and information systems by customers and partners must be controlled, and appropriate security practices must be established. Customers and partners must be informed of the access rules and conditions before being granted access. These rules and conditions should cover:

    1. Clear identification of information, information systems, or authorized areas for customer and partner access.

2. Specification of relevant rules, policies, procedures, and practices of the Company.
3. Specification of methods for controlling access and usage, such as the use of user accounts and passwords, including access rights of customers and partners.
4. Reporting procedures in case of abnormalities.
5. Specification of the Company's rights to audit and revoke access rights of customers and partners.

- Access rules and conditions for accessing data and information systems by customers and partners must be reviewed by the Information Technology Security team or the designated authority.
- Access to data and information systems by customers and partners must be appropriately monitored to prevent unauthorized modifications, alterations, or any actions that may cause damage to the Company's data and information systems.

3. Reviewing and Updating Policy

Information Security Policies, procedures, and any other guidelines shall be reviewed and updated by management at least once a year to ensure that its content is complete, effective, and can be used appropriately.

4. Penalties

Any breach, violation, negligence, or non-compliance with the policy, work instruction, and relevant supporting documents whether intentional or not, the Company may consider penalties at its discretion or disciplinary action in accordance with the Company’s policies. Any breach or violation of the policy is deemed to be an illegal act, the Company may consider further legal proceedings.

(The policy shall be effective as of 22 August 2023 onwards.)