Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

Information Security Basic Policy

TRANSACTION Group (hereinafter, "the Group") recognizes protecting the information assets held by the Group from various threats such as unauthorized access, cyberattacks, and system failures, and strengthening information security across the entire Group, as one of its important management issues. The Group has established this "Information Security Basic Policy" as its approach to information security initiatives and will strive to maintain and enhance information security.

1. Purpose

This Basic Policy sets forth the Group's policy for establishing and operating an information security management system, with the purpose of protecting the Group's information assets from all threats, whether intentional or accidental, originating both inside and outside the company, and ensuring the stable continuation of business activities.

2. Scope of application

This Basic Policy covers the "information assets" handled by the Group in its business activities and is applicable to the Group's officers, employees, and other related parties (which means officers; permanent employees, non-permanent employees, contract employees, and part-time employees working under employment contracts; and individuals working at each Group company under dispatch contracts and business outsourcing contracts) (hereinafter, "Officers and Employees, etc.").

3. Definitions

"Information security" means protecting the information assets handled by the Group from threats to their confidentiality, integrity, and availability. This also includes cybersecurity.

"Cybersecurity" means taking measures necessary for the security management of such information, including the prevention of information leakage, loss, or damage, as well as measures necessary to ensure the safety and reliability of information systems and information communication networks, and ensuring such systems and networks are properly maintained and managed.

4. Information security framework

The Group has established a Compliance Risk Management Committee chaired by the President and Representative Director of TRANSACTION Co., Ltd. to oversee risk management, and will establish an information security framework centered on the management team and strive for continuous improvement and enhancement. We will also establish a framework to regularly audit these initiatives and strive for improvement.

5. Information security measures

(1) Protection of information assets

The Group recognizes the importance of all information assets it holds from the perspectives of confidentiality, integrity, and availability, and will strive to protect information assets appropriately under its information security framework.

(2) Establishment of related internal regulations and compliance with laws, etc.

The Group will establish related internal regulations to ensure the proper implementation of information security measures and ensure that Officers and Employees, etc. are well aware of their content. Violations of laws or internal regulations related to information security will be dealt with strictly.

(3) Information security education

The Group will continuously implement education and training to enhance information security literacy and ensure the proper management of the Group's information assets.

(4) Audit

The Group will conduct regular internal audits to check for compliance with this Basic Policy and related internal regulations.

6. Response to information security incidents

In the event of a security incident, the Group will respond appropriately in an effort to resolve issues promptly, investigate the root cause, and implement measures to prevent recurrence.

7. Business continuity management

The Group will do its utmost to minimize business interruptions caused by information system-related disasters, failures or errors, or intentional misuse of information assets, etc., to ensure business continuity.

8. Continuous improvement

The Group will continuously improve its information security management by regularly evaluating and reviewing the initiatives outlined in this Policy.

Last updated on October 8, 2025