Security Policy (Basic Policy)

I Company Statement

This Security Policy sets forth the Company's basic policy on security measures for information assets (defined in II 2-1). It includes the necessary instructions for maintaining the security of internal information and is aimed at achieving the appropriate protection and utilization of all information assets held by the Company.

Officers and all employees must strive to ensure and support the effective functioning of the Security Policy.

II Information Assets

2-1. Information assets

Information assets refer to internal information (trade secrets, confidential information, general information, and other useful information), information systems that record, store, or transmit such internal information, and the internal frameworks necessary for the proper protection and utilization of such information and systems. In other words, they include not only business information (development information, customer information, etc.), internal documents, various types of data files, networks, hardware, and software that are necessary or useful for business operations, but also the personnel, etc. needed to manage and utilize confidential information and to develop and operate systems.

They are important assets of the Company, and if their legitimacy, reliability, or confidentiality were to be compromised, there would be significant potential for the Company to incur business losses. For this reason, the Company must appoint administrators of these assets to manage them properly in accordance with their importance to eliminate damage from various threats such as misuse, loss, destruction, failure, mishandling, disaster, theft, and leaks.

2-2. Access to information assets

To ensure that information assets are used appropriately for their intended purposes, the Company permits access only to those who have a legitimate need. To achieve this, the Company allocates the time and resources necessary to manage and monitor access to its information assets.

2-3. Confirmation by the Company

The Company is required to confirm that information assets are properly managed, protected, and utilized. For this reason, the Company regularly conducts investigations and requires reports on these matters.

2-4. Decisions made by the Company

Decisions made by the Company must not conflict with the proper use and protection of information assets. All officers and administrators must not instruct employees to engage in any acts that violate the Security Policy.

III Security Management Frameworks

3-1. Company-wide security management

The Company designates the Legal Department as the general security management division to maintain and manage security from a company-wide, consistent perspective and to establish the necessary security management frameworks.

The Legal Department is responsible for establishing the Security Policy and various regulations regarding security and ensuring that the Policy and those regulations function effectively.

3-2. Security management in individual departments

Each department appoints its own security manager. Security managers are responsible for the utilization and proper management of information assets in their own departments.

The security manager of each department appoints a security supervisor for that department. The security supervisor has a duty to communicate, maintain, and manage security measures in their department and to ensure that those measures function effectively.

The Legal Department supervises and supports each department's management of information assets.

3-3. Monitoring framework

The Auditing Department investigates and reports on whether each department is complying with the Security Policy and the arrangements and procedures that are based on the Security Policy.

IV Participation and Obligations of All Employees

4-1. Obligations of officers and employees

All officers and employees must participate in the implementation of security measures for information assets.

All officers and employees have a duty to implement procedures compliant with the Security Policy and to ensure that security measures function effectively.

4-2. Prevention of violations

The Company develops a system to prevent and deter violations of security measures for information assets. In the event of a violation, the person who committed the violation and the relevant security manager will be punished in accordance with laws and regulations, work regulations, etc.

V Compliance with Laws and Regulations Concerning Information Assets

Officers and employees comply with and follow laws and regulations and internal rules, etc. concerning information assets used in the execution of their duties. The security manager of each department is responsible for informing department personnel about relevant laws and regulations, and the Legal Department supports such efforts.