

Basic Policy on Information Security

Recognizing the importance of protecting and utilizing information assets, we, the Yoshida Group, commit to ensure security of information assets that we have decided to manage from threats such as accidents, disasters and crimes, and to live up to the trust of our customers and society.

1. Responsibility of Management

Under the leadership of its management, we will make efforts to improve information security institutionally and continuously, taking internal and external situations into account.

We will strive to prevent information security incidents. In case of incident occur, prompt action such as minimizing damage, preventing recurrence, and recovery shall be deployed.

To ensure full awareness of the importance of information security, necessary training will be provided to all directors and employees.

2. Organization of Internal System

In order to maintain and improve information security, we shall establish an organizational structure and formal internal regulations concerning information security measures, and shall implement information security management appropriately.

3. Efforts by employees

To ensure confidentiality, integrity, availability and protect information assets from various risks and threats, such as leakage, falsification, loss, destruction and interference with use, our employees shall acquire necessary knowledge and skills, solidifying our commitment to information security.

4. Compliance with laws, regulations, and contractual requirements

We comply with all applicable laws, regulations, codes, and contractual obligations related to information security, and shall live up to the trust of our customers and society.

5. Response to Violations and Accidents

In the event of any violation of laws and regulations, breach of contract, or accident related to information security, we will take appropriate measures to prevent recurrence.



October 1, 2023
Yoshida Group