The Kawasaki Group Policy on Information Security

1. Fundamental Concepts

The Kawasaki Group recognizes that the ensuring of information security to safeguard the information of customers and other business partners, protect our brand value, and avoid any impact on our business activities is a social responsibility of the company, and we believe it to be an important management issue relating to business continuity. As outlined below, our Group has stipulated an Information Security Policy and conducts proper operations in our business activities so as to manage and protect information handled by our Group as an important asset.

2. Policy on Information Security

(1) Objective and scope of application

The purpose of the policy is to enable all officers and employees of the Kawasaki Group to properly recognize the importance of information security and act accordingly. The policy applies to all business activities of the Group.

(2) Compliance with laws and regulations and fulfillment of contractual obligations

The Kawasaki Group will observe laws, ordinances, regulations, and other norms relating to information security, as well as contracts with business partners.

(3) Information security management structure

To implement even more appropriate information security countermeasures in our global and increasingly complex business activities, and to safeguard the trust, security, and safety of the Group’s customers and society at large, we will establish a management setup to realize organized and continuous operations relating to information security, thereby endeavoring to ensure information security.

We will establish the Supervisory Department headed by the officer in charge of information security as a head office organization and strengthen information security in cooperation with responsible departments in Group companies, related companies, and other business entities. Furthermore, in conjunction with the risk management department, we will regularly report on the state of implementation of information security measures to the Management Committee.

(4) Implementation of education and training

The Kawasaki Group will continuously conduct education and training on information security

required in their work for all officers and employees and promote the entrenchment of information security policies and awareness raising. In addition, in conjunction with responsible departments in Group companies, related companies, and other business entities, the Supervisory Department will implement drills simulating attacks from outside the company, thereby endeavoring to enhance our detection, response, and recovery capabilities against the latest cyber threats.

(5) Ongoing improvement of information security management

By formulating an information security strategy, conducting the planned deployment of measures, and implementing internal audits, the Kawasaki Group will regularly inspect and assess the state of management and operation and make continuous improvements. In addition, we will endeavor to maintain information security management by making positive use of assessments by professional bodies; collecting, evaluating, and analyzing information on threats to our business; and constantly implementing optimum countermeasures.

In conjunction with the legal affairs and compliance departments, the Supervisory Department will respond firmly to each country's laws and regulations relating to information management and build a setup that contributes to the expansion of global business.

(6) Response when problems occur

In the event of an information security incident occurring, the Kawasaki Group will respond swiftly to minimize damage, investigate the cause, and take steps to prevent any recurrence.

The Supervisory Department will endeavor to further strengthen its structure by setting up a dedicated department in charge of detection, response, and recovery relating to cyberattacks against our Group. In the event of a serious information security incident, this department will swiftly share information with the officer in charge and promptly report to business partners, related government ministries, and related organizations.

Established in September 2021
Revised in November 2021
Revised in August 2022