Kawasaki Group Policy on Information Security

1. Fundamental Concepts

The Kawasaki Group considers ensuring robust information security to be an integral part of its corporate social responsibilities and, therefore, believes that information security constitutes an important management issue affecting its business continuity. With this in mind, the Group has established the basic policies on information security listed below to ensure that all informational assets handled by the Group are managed as important assets and protected. The Group will thus practice these policies appropriately in the course of business activities.

2. Policies on Information Security

(1) Objective and Scope of Application

The objective of these policies is to ensure that Kawasaki Group officers and employees properly understand the importance of information security in business activities and act accordingly. Therefore, these policies apply to all the business activities undertaken by the Group.

(2) Compliance with Laws and Regulations and Fulfillment of Contractual Obligations

The Kawasaki Group will comply with laws, regulations, rules, and standards related to information security as well as fulfill its contractual obligations to customers.

(3) Information Security Management Structure

The Kawasaki Group will develop a management structure enabling the organizational adoption and continuous practice of information security measures in an effort to ensure robust information security.

Specifically, the Cyber Security Control Division, a body tasked with supervising all relevant security matters and headed by an officer in charge of cyber security, will be put in place at the head office and act in collaboration with divisions charged with cyber security management at internal companies to ensure the continuous strengthening of information security. Moreover, the Division will work in tandem with the Risk Management Department at the head office to provide the Management Committee with periodic reporting on the status of implementation of information security measures.

(4) Response to Problems

In the event that an information security incident emerges, the Kawasaki Group will promptly take action to minimize the resulting damage and investigate the causes of such incident in order to implement measures aimed at preventing recurrences.

To this end, the Cyber Security Control Division will maintain a cyber-defense center tasked with detecting, responding to, and spearheading recovery from cyberattacks against the Group, with the aim of securing an even stronger cyber security structure. In the event that the emergent security incident is serious, an officer in charge of cyber security will be immediately notified of such incident.

(5)Education and Training

The Kawasaki Group will regularly provide officers and employees with

information security education and training that addresses their varying needs based on their duties, thereby helping them raise their information security awareness.

The Cyber Security Control Division will act in collaboration with divisions charged with cyber security management at internal companies to conduct drills involving mock cyberattacks from outside the Group in order to secure greater capabilities for detecting and countering the latest modes of cyberattacks.

(6)Ongoing Improvement of Information Security

The Kawasaki Group will formulate cyber security strategies and systematically translate such strategies into security measures while implementing internal audits to periodically inspect and evaluate the status of information security management and practices, with an eye to achieving ongoing improvements. Also, the Group will proactively utilize information security assessment services provided by specialist organizations to ensure it attains and maintains a security level that satisfies the global standard.

Moreover, through collaboration between the Cyber Security Control Division and departments in charge of legal affairs and compliance, the Group will maintain proper compliance with information security-related legal regulations enforced in countries in which it operates. In these ways, the Group will secure a robust information security platform capable of supporting the expansion of its global operations.