Information Security Policy

1. Purpose

Based on “the HINO Credo” and “HINO Code of Conduct”, Hino Motors, Ltd. (hereinafter called “HML”) and HML’s consolidated subsidiaries (hereinafter collectively called “Hino”) understand that Information; such as trade secrets and personal information; created by Hino or received from customers, business partners or other entities in the course of business activities, associated information management systems and the control systems of Hino’s products and facilities (hereinafter called “Information Assets”) are critical assets for Hino’s business activities.

Based on the above understanding, HML establishes Information Security Policy (hereinafter called “The Policy”) to ensure that Hino manages and practices information security methodically and continuously.

2. Hino’s basic approach to information security

1) Compliance

Hino shall comply with applicable laws, governmental guidance, contractual obligations and other social norms related to information security.

2) Maintenance of stable business infrastructure

Hino shall ensure competitiveness and business continuity through the management and protection of its Information Assets.

3) Providing safe products and services

Hino shall incorporate information security practices into Hino’s business activities such as the development, design and production processes of products and services in order to provide safe products and services to customers.

4) Contribution to the establishment of safe Cyberspace

Hino shall act as a good corporate citizen by contributing to a safe online environment (“Cyberspace”) by working to identify and mitigate information security vulnerabilities in Hino’s Information Assets.

5) Information Security Management

Hino shall continuously implement information security management through the establishment of governance and risk management including incident response.