Information Security Guidelines

1.Legal compliance

We comply with laws and regulations related to information security, national guidelines, contractual obligations, and other social norms.

2.Maintaining a stable business foundation

We strive to maintain a stable business foundation, ensuring competitiveness and business continuity, by appropriately managing and protecting information assets.

3.Providing safe products and services

We provide safe products and services to our customers and society by taking information security measures in our own business activities, including the development, design, and manufacturing of products and services.

4.Contributing to creating a safe cyberspace

We will contribute to the creation of a safe cyberspace so that users can enjoy its benefits with peace of mind.

5.Information security management

We will build a governance system, conduct risk management including accident response, and continuously promote and improve information security.

6.Strengthening the responsibility system

In order to appropriately manage and protect information assets, we will establish an information security promotion system and clarify its duties and responsibilities.

7.Preparation and compliance with information security regulations

We will formulate and comply with information security regulations based on these Guidelines.

8.Risk assessment

(1) We identify information assets to be protected and information security threats to them.

(2) We will take necessary measures to prevent the occurrence of events that compromise the confidentiality, integrity, or availability of information assets, based on the status of preparedness against identified threats and the degree of impact of the threats.

(3) In the event that an information security incident occurs, we will promptly take appropriate measures to bring the incident under control, restore the situation to its original state, prevent the spread of damage, and prevent recurrence.

9.Education and awareness

We will carry out necessary education and awareness-raising activities to raise awareness of information security among executives, employees, etc.

10.Continuous improvement

We implement the PDCA cycle in information security and continually review and improve information security mechanisms.

11.Inspection and audit of initiative status

We shall conduct regular inspections and audits (including internal audits) regarding the status of initiatives based on these Guidelines, and report the results to management.

2023.10

CATALER CORPORATION

CATALER