Information Security Basic Policy

AISIN Group Information Security Basic Policy

The AISIN Group lays down the AISIN Group Information Security Basic Policy (the "Policy") to ensure information security systematically and continually with understanding that information assets deposited by customers and business partners or possessed by the Group regarding its business activities ("Information Assets") are an important property of the Group.

1. Basic Stance

(1) Legal compliance

The Group complies with laws and regulations, government guidelines, contractual obligations, and other social norms regarding information security.

(2) Maintenance of stable financial and managerial base

The Group commits itself to maintaining a stable financial and managerial base with competitive strength and business continuity through proper management and protection of Information Assets.

(3) Provision of safe products and services

The Group takes information security measures in its business activities, including product and service development, design, manufacturing and marketing, to provide customers and society as a whole with safe products and services.

(4) Contribution to building secure cyberspace

The Group contributes to building a virtual space, where diverse services and communities are created, on the Internet that consists of information systems and information communications networks and distributes information ("Cyberspace") so as to ensure that users can rest assured in enjoying the benefits of Cyberspace.

(5) Information security management

The Group develops a governance framework and implements incident response and other risk management measures to continuously promote and improve information security.

2. Information Security Efforts

(1) Clarification of duty and responsibility structure

The Group develops a promotion structure to clarify duties and responsibilities in information security for ensuring proper management and protection of Information Assets.

(2) Development of information security regulations

The Groups establishes information security regulations and develops specific management guidelines and procedures based on the regulations.

(3) Risk management

[1] The Group identifies Information Assets to be protected and information security threats to them.

[2] The Group takes necessary measures to prevent events that may damage the Information Assets based on the status of readiness for and possible impact of the identified threats.

[3] If an event occurs that damages the Information Assets, the Group will promptly take appropriate action to contain the event, prevent the damage from spreading, restore the Information Assets to their original state, and prevent recurrence of such events.

(4) Education and awareness building

The Group provides officials and employees with necessary education and awareness activities to raise their awareness of information security.

(5) Continuous improvement

The Group implements an information security PDCA cycle to continuously review and improve the information security structure.

3. Inspections and Audits of Ongoing Efforts

The Group conducts periodical inspections and audits (including internal audits) of efforts ongoing in accordance with the Policy and reports the results of them to the leadership in charge of risk management.

January 2022
AISIN CORPORATION
Chief Software & Digital Officer