Information Security Management Policy

Unit in charge: Information Security Department
Time of first drafting: April of 2006
Date of announcement:2019.10.04

Article One
In order to maintain the overall information security of the enterprise, to strengthen the security management of various information assets, and to ensure the confidentiality, integrity and availability of these assets, so as to maintain the sustainability of this company, we have drafted our Information Security Management Policy (hereinafter the Policy).

Article Two
This policy applies to the company's various information operations, information assets and information users, including employees, temporary employees, visitors who do business with the company (including their employees, temporary employees, etc.) as they maintain, hold, use, and manage the Company’s information assets

Subsidiaries that are regulated by Article 2 of the Company's "Subsidiary Supervision Derivatives" shall, according to their scale of operations, nature of business, managerial needs, and characteristics of risks, establish relevant regulations and establish appropriate management mechanisms with reference to this policy.

Article Three
Important nouns used in this policy are defined as below:

1. Information assets: information assets are assets that are used in the collection, generation, and employment of information or related assets that are also needed to accomplish these operations, including but not limited to personnel, equipment, systems, information, data, networks and the environment.
2. Information users: information users refer to full-time employees, contracted employees, hardware installation and maintenance vendors, and other persons authorized to use information assets.
3. Threats: situations or events sufficiently capable of causing harm or damage to information assets.
4. Weaknesses: elements that are found in the inherent design of the external environment of the information assets and are potentially vulnerable to threats and the ensuring damage
5. Interested parties: individuals or organizations that can objectively or subjectively think they can affect or be affected by information-related policies or activities.

Article Four
The information security goals and information security control measures are as follows:

1. Information Security Goals
   (1) Ensure the confidentiality of the company's information assets and implement data access control.
   (2) Ensure the integrity of the company's information operations management and avoid unauthorized modification.

(3) To ensure that the company's information operations continue to operate, meet operational service standards, and reach applicability standards.
(4) Ensure that the company's information operations meet the requirements of relevant laws and regulations.

2. Information security control measures
(1) Establish an information security management organization, supervise the operation of the information security management system, and identify internal and external issues of the information security management system and the requirements and expectations relevant interested parties hold for this Company regarding information security.
(2) The management team shall commit itself to maintaining information security, continuously improving the quality of information security, and reducing the occurrence of information security incidents in order to protect the rights and interests of customers.
(3) As an integral part of the information security management system documents, information security indicators should be updated, drafted, and tested at appropriate intervals; projection of records shall be conducted with a clear management mechanism.
(4) All personnel of the company have the responsibility and obligation to protect the information assets they own, hold or use; training and promotion of employee information security risk awareness and knowledge of the laws and regulation shall be executed regularly.
(5) Full-time and part-time employees of vendors that do business with the Company shall comply with the information security regulations of the Company.
(6) To ensure the effectiveness of information security controls, asset inventory operations, access control requirements, communication security management, and workplace safety should be regulated. It is also necessary to standardize the information operations of external units regarding what safety issues should be focused on and specify the scope of responsibility of external personnel.
(7) The development, modification and establishment of information operations or procedures shall be handled in accordance with regulations, and at the same time, the operation continuity plan shall be set according to the actual needs of business execution.
(8) Information security incidents and violations of security policies and regulations shall be reported in accordance with procedures.

Article Five

This policy must be reviewed once a year and will be changed in accordance with relevant laws, business development status, internal and external environments and other factors; if need be, it will also be appropriately modified to ensure the effectiveness of this policy.

Article Six

This policy will take effect from the date of its release after being approved by the board of directors, as is the case when this policy is amended.