Phison Information Security Policy

First, the purpose:

To enhance the confidentiality, integrity and usability of the information assets, Phison Electronics Corp. (hereinafter referred to as the Company), in order to strengthen the management of the Company, to provide the information environment for continuous operation of the Company's business and to comply with relevant government regulations and internal and external stakeholders to avoid any internal and external deliberate or accidental threats to achieve information security.

Second, the scope:

The information security management system of the Company is set up for the safety management of computer facilities maintenance, business operation and website maintenance, and has fully grasped the information operation and management process, and satisfies the safety requirements and expectations.

Third, the definition:

Information assets: refers to the hardware, software, services, documents and personnel that maintain the operation of the Company's information business.
Confidentiality: Ensure that only authorized users have access to information
Integrity: to ensure that information and processing methods are correct and complete
Usability: Ensure that authorized users have access to information and related assets when needed
The information environment for continuous operation of the business: the computer operating environment required to maintain the operation of the Company's business.

Fourth, the goal:

Maintain the confidentiality, integrity and usability of the Company's information assets and protect the privacy of our users. Through the joint efforts of all colleagues to achieve the following objectives:

1. To protect the company's business information, to avoid unauthorized access, modify, and to ensure its correct and integrity.
2. With respect to intellectual property rights, protect customers and company information.
3. To ensure that all information security incidents or suspicious security weaknesses should be reported, and investigated and processed properly.
4. To meet the requirements of relevant laws and regulations, to achieve the goal of continuous operation of business.

Fifth, the responsibility:

1. All colleagues should participate actively and support the information security management system, and implement the policies and procedures according to appropriate standards and procedures.
2. All personnel, organizations, service providers, outsources and visitors related to business operation are required to comply with this policy.
3. All colleagues and outsourced service providers have the responsibility to report the information security incidents or weaknesses.
4. Any action that jeopardizes the information security shall be punished in accordance with the relevant provisions of the Company, or made accountability subject to the severity of their civil, criminal and administrative liability.

President AYCK