

Information Security Policy

1. Purpose

In order to ensure the safe operation of personnel, data, systems, equipment and networks related to information operations of Advantech Co., Ltd. (hereinafter referred to as the company), and to comply with the requirements of relevant laws and regulations, an information security policy (hereinafter referred to as this policy) has been formulated as the highest guiding principle.

2. Scope

- (1). It is applicable to the security management of the company's information assets, covering its confidentiality, integrity and availability.
- (2). All employees, contractors, consultants, temporary employees, customers, and third-party personnel involved in the company's information operations or data use should follow this policy.

3. Management Principles

- (1). Establish an information security organization and specify its rights and responsibilities to promote and maintain related management, execution, and inspection tasks.
- (2). Formulate information security management related methods and procedures to protect the confidentiality, integrity and availability of personnel, data, systems, equipment and networks.
- (3). Convene information security management meetings on a regular basis to review the latest status in internal and external risks, technology and business needs, and take corresponding measures.
- (4). Regularly conduct various information security testing and audits to assess the risks of the information environment and make improvements.
- (5). Deploy information security protection systems and monitoring equipment to continuously improve the security of the overall information environment and reduce the security incidence.
- (6). The use of the system and data must be authorized, and the granting of access rights should be based on the minimum scope required by the business.

- (7). Establish appropriate system architecture and backup mechanisms and conduct contingency exercises to strengthen the resilience of information services.
- (8). Establish response and notification procedures for information security incidents to enhance employee's ability to respond and coordinate in the face of emergencies.
- (9). Conduct information security education and training for employees, and continue to enhance employees' awareness.
- (10). In accordance with the regulations of information security and personal information protection, handle and protect the security of data and systems carefully.

4. Review

- (1). This policy should be reviewed at least once a year to reflect the latest developments in relevant laws, technology and the company's business, and be appropriately revised.
- (2). The revision of this policy is approved by the general manager, and become effective on the announcement day. In addition, interested parties, such as all employees, cooperating manufacturers, suppliers, etc., shall be notified by announcement, writing, e-mail or other methods.