Wistron Corporation
Information Security Policy

Article 1 Objective

In order to protect various types of information related to Wistron Corporation (hereinafter referred to as the Company), its products, and services, avoid unauthorized access, modification, use and disclosure, and uphold the information security management mission of "building a resilient, secure and trustworthy enterprise", the "Information Security Policy" has been formulated for compliance, and the establishment of a sound information security management mechanism to ensure compliance with relevant laws and regulations and maintain the stability and continuity of the company's business operations, protect customer assets and confidential information, thereby enhancing customer trust and fulfilling our responsibilities and commitments to shareholders and stakeholders.

Article 2 Scope

Our global employees, suppliers and customers who enter our premises.

Article 3 Organization and Authority

3.1 The Board of Directors serves as the highest decision-making unit for promoting information security policies, and has established the Sustainability Development and Information Security Committee under the Board of Directors to formulate the Company's information security development direction, strategy and goals.

3.2 The Information Security Executive Committee meets quarterly and may hold an extraordinary meeting if necessary, and the agenda of the meeting includes:① information security incident handling reports, ②reports on the progress of internal affairs of each group, ③matters requiring the cooperation of various units of the company, and④ other relevant suggestions or extempore motions.

3.3 Each Company's overseas manufacturing facilities have established their own information security executive committees, which operate according to local conditions and cooperate with the Company in promoting the implementation of information security strategies and strategic plans.

Article 4 Information Security shall be Jointly Maintained by all Employees of the Company

4.1 All employees of the Company should pay attention to any possible information security risks and report them to the information security committee in accordance with the information security procedures.

4.2 The information security unit shall be responsible for establishing defense mechanisms and assisting in the elimination of information security

incidents to ensure the company's information security.

4.3 The Company regularly organizes employee information security and personal data protection education, training, and publicity, and provides appropriate training topics according to different positions, establishes information security knowledge and data protection awareness of all employees, and strengthens the responsibility of all employees to protect personal information.

Article 5 Ensure data integrity and implement information security protection control mechanisms

5.1 In order to ensure the accuracy of the information content, the Company implements an in-depth information security defense mechanism to prevent unauthorized access, falsification, or destruction.

5.2 The Company has established data governance and software security development control mechanisms to ensure that data is subject to control measures throughout its life cycle to prevent data leakage and ensure that only authorized users can modify or access sensitive information.

Article 6 Continuously monitor and respond to information security threats

6.1 The Company shall establish an information security incident response organization, set up an incident notification mechanism, integrate internal information security personnel and external information security expert resources, actively monitor network security risks, respond quickly to incidents, and implement mitigation strategies.

6.2 In the event of an information security threat, the Company shall implement a hierarchical reporting process and response mechanism according to the level of information security incidents, notify the affected stakeholders, conduct incident investigation, handling, and improvement reports, and explain in detail the actions taken to address the vulnerabilities and measures to prevent future risks in the report.

Article 7 Continuously optimize the information security system

7.1 The company should adopt international information security governance standards and frameworks, align with international standards, keep pace with the times, continuously improve management actions, regularly conduct information security risk assessments, and invest necessary resources (including equipment, tools, people, services, etc.) to ensure that risks are controllable.

7.2 The Company regularly conducts internal and external audits, and entrusts external third-party information security experts to conduct red team drills and penetration tests to review the overall information security work environment to ensure effective operation and continuous improvement of

control measures.

Article 8 Strengthen third-party information security requirements

8.1 The Company's third parties (including but not limited to suppliers, etc., hereinafter referred to as "third parties") shall comply with the Company's Information Security Policy.

8.2 Our contracts with third parties must include information security clauses to ensure the integrity and confidentiality of our data.

8.3 The Company formulates third-party hierarchical management principles based on the security, risk, and privacy aspects of third parties, as well as the level of confidentiality of access data, conducts hierarchical control of third-party information security, and regularly conducts third-party risk assessments to ensure that third parties implement the information security management principles required by the Company.

8.4 A third party shall be required to notify the Company of major information security incidents and continuously report on improvements.

Article 9 Management commitment

The Company's information security management aims to ensure the sustainable operation of the company, and the Company shall provide necessary resources for the operation of the information system and security management system to minimize losses by preventing and reducing the impact of information security incidents.

Article 10 Implementation and review

The Company always pays attention to the latest developments in information security management at home and abroad, and regularly reviews and adjusts this information security policy accordingly to improve the effectiveness of information security management and comply with relevant laws and regulations.

Article 11 Take effect

This policy shall be implemented after being approved by the board of directors, and the same shall apply when amended.

This policy was established on August 12, 2025.