TSC Auto ID Technology Co., Ltd.

Personal Data Protection Policy and Implementation Report in 2025

The company values personal data protection and follows the "Personal Data Protection Act." We have established and announced the implementation of the "**Personal Data Protection Management Rules**" as the basis and operating procedures for collecting, processing, using, and internationally transferring personal data, ensuring the security of personal information.

1. Policy Disclosure and Management Mechanism

   The company's " **Personal Data Protection Management Rules**" cover the subjects and scope, responsibilities, operating principles, emergency response procedures and complaint channels, technical and organizational security measures, as well as liabilities and penalties for violations. These regulations are approved by the board of directors and are updated as needed.

   The HR department signs a 'Personal Data Collection Consent Form' and a 'Confidentiality Agreement' with each employee. These documents specify the purpose, scope, and method of personal data collection, as well as the rights of the individuals involved, and written consent is obtained in accordance with the law. They also fulfill their duty of confidentiality.

   The company obtained ISO27001 Information Security Management System certification in 2025 (valid from 2025/12/29 to 2028/12/28), and we implement strict cybersecurity measures across hardware, software, and staff operations.

2. Scope of Application and Responsible Departments

   Object: This applies to all company personnel, vendors or consultants who have business dealings with the company (including their employees or temporary staff), job applicants, and visitors to the company.

   Scope：This policy protects the personal data safeguarded by the Personal Data Protection Act. It sets regulations for the collection, processing, use, and international transfer of personal data to ensure data security.

   Responsibilities:

   1. All Employees：Understand and fully comply with this policy, and actively participate in its implementation.

2. Human Resources Department：The personal data protection management organization is responsible for overseeing the operation of the company's personal data management system, managing and directing the implementation of the company's personal data protection efforts, and ensuring compliance with this policy.

3. Department Supervisors：As members of the personal data protection management implementation team, they are responsible for drafting and promoting policies, planning, implementing, operating, monitoring, auditing, maintaining, and improving the personal data management system, and reviewing it periodically or whenever major changes occur to ensure its appropriateness and effectiveness.

3. Implementation Status

The company has achieved the following concrete results in terms of systems, training, and technical management:

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>1</td><td>Percentage of employees who signed the 'Personal Data Collection Consent Form'：100%</td></tr>
<tr><td>2</td><td>Percentage of employees who signed the 'Labor Confidentiality Agreement'：100%</td></tr>
<tr><td>3</td><td>No incidents of personal data protection violations occurred</td></tr>
<tr><td>4</td><td>Information on employee completion of personal data protection training is as follows:
<table>
<tr><th>Course</th><th>No. of Participants</th><th>Hours</th></tr>
<tr><td>Introduction to Law and Life</td><td>27</td><td>27</td></tr>
<tr><td>Email Security and Social Engineering Prevention (2025)</td><td>97</td><td>194</td></tr>
<tr><td>Analysis of Network Attack Techniques</td><td>199</td><td>398</td></tr>
</table></td></tr>
</table>

4. " Personal Data Protection Management Rules"

[note: In the event of any discrepancy between the English version and the original Chinese version or any differences in the interpretation of the two versions, the Chinese-language Personal Data Protection Management Rules shall prevail.]

Article 1 Purpose

These Regulations are established to implement the Company's personal data protection management system and to ensure compliance with the Personal Data Protection Act. (hereinafter referred to as the "PDPA").

Article 2 Scope and Applicability

2.1 Applicable Parties

These Regulations apply to all personnel of the Company, vendors and consultants having business relationships with the Company (including their employees and temporary staff), job applicants, visitors to the Company, and other relevant persons.

2.2 Scope

These Regulations apply to personal data protected under the PDPA. They establish the requirements governing the collection, processing, use, and international transfer of personal data to ensure the security and protection of such personal data.

Article 3 Definitions

3.1 Personal Data Management System

A risk-based management system established for the purpose of implementing, operating, monitoring, reviewing, maintaining, and continually improving the Company's management of personal data.

3.2 Personal Data Management Metrics

Measures established to evaluate the effectiveness of selected controls in achieving the Company's personal data management objectives.

3.3 Purposes for the Collection of Personal Data

The Company may collect personal data for the following purposes:

Products and services, Business operations, Communications and marketing, Information system management, Supplier management, Health and safety, Asset security, Surveys and feedback, Corporate security, Investigation of incidents or cases, Legal and regulatory compliance, Improvement of the Company's websites, products, and services, Fraud prevention, Establishment, exercise, or defense of legal claims or rights, and Recruitment and interview processes.

3.4 Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person, including but not limited to name, date of birth, national identification number, passport number, characteristics, fingerprints, marital status, family information, education, occupation, medical records, medical information, genetic information, sexual life, health examination records, criminal records, contact information, financial status, social activities, and any other information that may

directly or indirectly identify a specific individual.

Should the competent authority amend the definition or scope of personal data under applicable laws or regulations, such amended definition and scope shall prevail.

3.5 Sensitive Personal Data

"Sensitive Personal Data" means personal data relating to medical records, genetic information, sexual life, health examination records, and criminal records.

Should the competent authority amend the definition or scope of sensitive personal data under applicable laws or regulations, such amended definition and scope shall prevail.

Article 4 Responsibilities

4.1 All Employees

All employees shall understand and strictly comply with these Regulations and shall fully participate in the implementation of the Company's personal data protection program.

4.2 Human Resources Department

The Human Resources Department shall serve as the Personal Data Protection Management Organization. It shall be responsible for overseeing and supervising the operation of the Company's Personal Data Management System (PDMS), directing and coordinating the implementation of the Company's personal data protection management activities, and ensuring compliance with these Regulations.

4.3 Heads of Departments

Department heads shall serve as members of the Personal Data Protection Management Organization and shall be responsible for formulating and promoting this Policy, as well as planning, implementing, operating, monitoring, auditing, maintaining, and continually improving the Personal Data Management System (PDMS). The PDMS shall be reviewed periodically or whenever significant changes occur to ensure its continued suitability and effectiveness.

Article 5 Operating Procedures

5.1 Scope of Personal Data Protection Management

The Company's personal data protection management shall be established in accordance with its business scale and operational characteristics and shall include, but not be limited to, the following:

5.1.1 Establishment of Personal Data Protection Management Procedures. The Company shall establish personal data management procedures in accordance with applicable information security standards and the requirements of the Personal Data Protection Act.

5.1.2 Principles Governing the Collection, Processing, and Use of Personal Data. Personal data shall be collected, processed, and used only for specific lawful purposes and only to the extent necessary. The following principles shall apply:

5.1.2.1 The specific purpose for collecting personal data shall comply with applicable laws and regulations, and appropriate audit trails shall be retained.

5.1.2.2 The processing of personal data shall comply with the Company's Information Security Policies. Appropriate access authorization, data classification, risk levels, and corresponding control measures shall be established.

5.1.2.3 Notification obligations shall be fulfilled by determining whether notification may be exempted under applicable laws and, where required, providing appropriate notices based on the circumstances of collection.

5.1.2.4 The Company shall ensure that personal data are used only for the specified purposes. Any use beyond such purposes shall comply with applicable legal requirements, and appropriate audit trails shall be maintained.

5.1.2.5 Except as otherwise permitted or required by applicable laws and regulations, the collection, processing, or use of Sensitive Personal Data is strictly prohibited.

5.1.3 Security Measures for Personal Data Files. The Company shall implement appropriate technical and organizational measures to safeguard personal data files and protect all personal data collected, processed, or used by the Company.

5.1.4 Collection of Personal Data：

Where personal data are collected, the Company shall obtain the data subject's consent where required, inform the data subject of the scope and retention period of the intended use in accordance with the PDPA and other applicable laws, obtain the relevant consent documentation, and securely retain such documentation together with the associated records. Personal data shall not be disclosed or used for purposes beyond those originally specified without proper authorization, thereby protecting the privacy rights of the data subject.

5.2 Personal Data Incident Response Procedures

5.2.1 The Company shall establish acceptable risk levels and corresponding response measures for personal data protection. Where a personal data incident results in

damage to the rights or interests of stakeholders, the Company shall respond appropriately and handle such incidents in accordance with its Information Security Policies.

5.3 Complaint Handling Mechanism

The Company shall establish channels through which data subjects may exercise their rights relating to personal data. Complaint handling shall also be conducted in accordance with the Company's Whistleblower Reporting and Protection Management Policy.

5.3.1 Complaint Email:tscwb@tscprinters.com

5.3.2 Address: 9F., No. 95, Minquan Road, Xindian District, New Taipei City 231023,

「TSC Auto ID Technology Co., Ltd. Internal Audit Office」

5.4 Continual Operation of the Personal Data Management System

5.4.1 The Company shall periodically evaluate and audit its personal data management procedures, Personal Data Management System (PDMS), and personal data management metrics to ensure the effectiveness of this Policy and related procedures and verify proper implementation.

5.4.2 Where deficiencies are identified or regulatory requirements are amended, the Company shall improve the relevant procedures and management measures to continually enhance the effectiveness of the Personal Data Management System.

5.5 Information Security

5.5.1 The Company has implemented appropriate technical and organizational security measures to protect the security of personal data. Individuals are requested to ensure that personal data are transmitted to the Company through secure means.

5.6 Retention of Personal Data

5.6.1 The Company shall make reasonable efforts to ensure that personal data are retained appropriately for the applicable statutory retention period or for as long as necessary to fulfill the purposes for which the data were collected.

5.7 Violations and Disciplinary Actions

5.7.1 All personnel of the Company shall comply with this Policy. Any violation shall be subject to disciplinary action in accordance with the Company's relevant rules and regulations.

5.7.2 **Where a violation gives rise to civil liability, criminal liability, or administrative penalties, the Company may, upon verification of the facts, terminate the employment or contractual relationship in accordance with applicable agreements or laws and pursue legal remedies as appropriate.**

5.7.3 **An employee's obligation to protect the Company's personal data shall survive the termination of his or her employment.**

Article 6 Implementation and Amendments

6.1 **Any matters not provided for in these Regulations shall be governed by the Company's relevant internal policies and applicable laws and regulations issued by the competent authorities.**

6.2 **These Regulations shall become effective upon approval by the Board of Directors. Any amendments hereto shall follow the same approval procedure.**