TCC Group Holdings CO., LTD.
Personal Data Protection and Management Policy

Article 1. Purpose and Basis

To protect and manage personal data which align with the Personal Data Protection Act (the "PDPA"), the Regulations for the Security and Maintenance of Personal Data Files by the Manufacturing and Technical Service Industries, and the Regulations Governing the Security and Maintenance of Personal Data Files Designated by the Financial Supervisory Commission for Non-Governmental Agencies (hereinafter referred to as the "FSC Regulations"), as well as the Company's internal control policies and standards, this Personal Data Protection and Management Policy (" The Policy") is enacted as the highest guidance for the Company.

Article 2. Scope

All employees of the Company, as well as personnel of client(s), supplier(s), contractor(s), external consultant(s), and other third-party shall be subject to the Policy.

Article 3. Definition

Section 1. Personal Data

"Personal Data" means any information relating to an identifiable natural person, such as the individual's name, date of birth, national identification number, passport number, physical characteristics, fingerprints, marital status, family background, education, occupation, medical records, medical treatment, genetic information, sexual life, health examination results, criminal records, contact details, financial status, social activities, or any other information that, directly or indirectly, can be used to identify that natural person. The definition and scope of Personal Data shall be revised in accordance with any amendments to applicable laws and regulations issued by the competent authority, and the revised definition and scope shall prevail.

Section 2. Sensitive Personal Data

"Sensitive Personal Data" means any information relating to medical records, healthcare, genetic information, sex life, physical examination results and criminal records.

Section 3. Data Subject

"Data Subject" means an individual whose personal data is collected.

Section 4. Other Terms
The definitions of other terms shall be as set forth in Article 2 of the PDPA.

Article 4. Management of Personal Data
Section 1
The collection, processing, and use of personal data shall be carried out in a way that respect the data' subject's rights and interests, , in an honest and good-faith manner, shall not exceed the necessary scope for the specified purposes, and shall have reasonable and legitimate connections with the purposes of collection.

Section 2
The personal data collected, processed, and used by the Company primarily consists of general personal data, including but not limited to, information relating to employees, customers and their employees, vendors and supply chain personnel. Unless necessary for business operations or required by law or regulations, the Company does not collect sensitive personal data.

Section 3
To respect Data Subject's rights, the Company is committed to applying the highest level of confidentiality and to conducting cross-border transfers under lawful, appropriate, and adequate safeguards.

Section 4
Where the collection, processing, or use the personal data is entrusted to a third party, the Company shall appropriately supervise the third party and shall ensure that the third party's data-protection rules and controls comply with applicable laws and regulations and with the Policy.

Section 5
The Company shall stipulate measures that enable Data Subjects to exercise their rights under Article 3 of the PDPA, including the procedures for submitting such requests, any fees payable, and the Company's mechanisms for reviewing and responding to those requests.

Section 6
The Company shall stipulate a responsible and protection unit ("Management Unit") staffed with designated personnel, and establish management systems for all personal

data-processing procedures, and provide the Management Unit's contact window and contact information so as to respond to Data Subjects' requests.

Article 5. Security and Maintenance of Personal Data

Section 1.

The Company shall ensure that proper security and maintenance measures are adopted for the collection, processing, or use of personal data in order to prevent theft, alteration, damage, loss, or leakage of such data. To protect the security and accuracy of personal data, the Company shall regularly review the security of its data-file systems.

Section 2.

To safeguard the security of stored personal data, the Company shall, in accordance with business necessity, define and limit the access rights of relevant personnel, monitor and control their actual access to such data, and require all personnel to comply with confidentiality obligations.

Article 6. Data Retention, Archiving and Improvement Mechanism

Section 1.

The Management Unit shall retain records or other evidence demonstrating the actual implementation of legally mandated personal-data management system and its related security and maintenance measures.

Section 2.

To continuously improve personal-data security and maintenance measures, the Management Unit or designated personnel shall review and revise personal data protection matters and regularly submit assessment reports.

Article 7. Personal Data Processing Procedure After Business Termination

To prevent theft, tamper, damage, loss or leakage of personal data, the Management unit shall, in accordance with applicable laws and regulations, establish procedures for processing personal data after the termination of business operation.

Article 8. Reporting Mechanism

To respond to data-security incidents such as theft, tempering, damage, loss or leakage of personal data ("Incidents"), the Company shall establish an emergency response plan and associated reporting and prevention mechanisms. These mechanisms shall include mitigation measures, identification of notification recipients, methods and content of notification, incident-response procedures, impact assessments, corrective and

preventive actions and post-incident sanctions.

Article 9. Management Unit

Section 1.

The Management Unit shall establish a risk assessment framework for the personal data management system and require individual department to regularly verify whether personal data processing procedures are carried out in accordance with applicable laws, regulations, and the Company's relevant policies and standards. The Management Unit shall also conduct risk assessments and implement improvements to the management system to ensure that the Company’s personal data protection practices comply with all relevant legal and regulatory requirements.

Section 2.

In addition to establish a management system in accordance with the Policy, the Management Unit shall proactively develop and promote personal-data protection guidelines, associated rules, and consent forms. In the event of any amendment of personal-data laws or regulations, the Management Unit shall promptly revise and implement the relevant guidelines, rules and documentation.

Article 10. Training and Zero-Tolerance Policy

Section 1

To ensure that the Company’s management of personal data complies with applicable laws or regulations, the Company shall regularly conduct training for all personnel on personal-data protection and management and shall evaluate the effectiveness of such training. The performance of trained personnel shall also be assessed, and the corresponding assessment records shall be retained.

Section 2, Article 10.

A Zero-Tolerance Policy toward any violation of personal data protection is adopted. Personnel who breach the relevant policies and rules will be subject to disciplinary action in accordance with internal personnel management regulations and employee disciplinary code. Depending on the seriousness of the circumstance, the matter shall be referred to the competent authorities for legal action under applicable laws.

Article 11. Complaint and Whistleblowing Mechanism

In a Data Subject becomes aware of an incident or circumstance involving damage to personal data, or any situation that may breach the Policy, the Company employees, external parties or any individuals may file a complaint or report through the hotline or

official email address established by the Management Unit. The Company shall strictly protect whistleblowers and safeguard their rights and interests.

Article 12. Implementation

The Policy shall take come into effect upon approval by the Board, and the same shall apply to any subsequent amendments hereto.