TCC Group Information Security Policy

I. Purpose

This policy is hereby established to build the TCC Group's information security management system to safeguard the confidentiality, integrity, and availability of its information assets. It aims to mitigate internal and external threats, ensure the stability of business operations, and fortify trust among stakeholders. Adhering strictly to international standards such as ISO 27001 and relevant regulations, while considering the specific business needs of TCC Group, this policy serves as the highest directive for its information security management framework.

II. Scope of Application

This policy applies to all TCC Group headquarters, domestic and international subsidiaries, and other affiliated entities under substantive control. It encompasses all employees, including contracted and dispatched personnel, as well as third-party partners, contractors, and suppliers who access the TCC Group's information assets.

III. Information Security Responsibilities

1. **Total Responsibility**
   All employees shall comply with this policy and all associated operational directives, assuming appropriate responsibilities for information security in accordance with their respective roles.
2. **Management Commitment**
   Management shall allocate the necessary resources and provide unyielding support for the effective implementation of the information security system.
3. **Third-party Compliance**
   All third-party personnel cooperating with the TCC Group are required to sign and adhere to the TCC Group's information security agreements and regulations, and shall not use or access the TCC Group's information assets without authorization.

IV. Information Security Governance

To ensure comprehensive oversight, the following structures are established:

1. **Information Security Management Committee:** This Committee operates under the ISO 27001 framework to promote information security policies, with a member of the Group's Board of Directors serving as Chair.
2. **Information Security Officer (CISO):** The CISO is entrusted with planning information security strategies, supervising their application, reviewing performance outcomes, and regularly reporting to the Management Committee.
3. **Policy Function:** This policy shall serve as the foundation of the TCC Group's information security management system; all relevant operational standards and procedures shall be derived therefrom.
4. Department heads are accountable for ensuring full adherence to this policy within their respective units.

V. Information Security Objectives

TCC Group shall pursue the following objectives to uphold its commitment to information security:

1. Ensure the confidentiality, integrity, and availability of information assets are continuously preserved and enhanced.
2. Safeguard information assets throughout their lifecycle, including creation, usage, storage,

transmission, and disposal, and prevent unauthorized access, modifications, disclosures, or misuse.

3. Implement protective measures to mitigate risks of malicious attacks, data breaches, service interruptions, and information leaks.
4. Comply with applicable laws, contractual obligations, international standards, and internal regulations.
5. Establish robust monitoring and reporting mechanisms to facilitate rapid operational recovery following security incidents or disasters.
6. Cultivate a culture of information security among employees, enhancing their awareness and accountability.
7. Manage information security risks effectively, ensuring risks remain within organizational tolerances through assessment and mitigation.
8. Regularly review policies, risks, control measures, and incidents to drive continuous improvements in security management effectiveness.

VI. Information Security Guiding Principles

1. **Personnel Awareness**
   - Conduct scheduled or ad-hoc training sessions and awareness campaigns on the latest threats and countermeasures in information security.
   - Exercise caution in handling sensitive information, ensuring it is not transferred to unauthorized devices or platforms.
2. **Technology and Procedures**
   - Ensure all systems and equipment are equipped with approved antivirus and protective software, regularly updated and patched to address vulnerabilities.
   - Employ encryption or other suitable protective measures to secure the transmission and storage of sensitive data.
3. **Monitoring and Incident Management**
   - Deploy active monitoring mechanisms to detect and analyze anomalies and threats.
   - Promptly report any security incidents to the Information Security Department in accordance with established reporting procedures and implement isolation and resolution measures as necessary.
   - Maintain transparency with affected internal and external stakeholders by disclosing the cause of incidents, actions taken, and improvement plans in a timely manner.
4. **Third-party Management**
   - Require partners and suppliers to adhere to the Group’s security policies and contract terms, and cooperate fully in information security audits.
5. **Continuous Improvement**
   - Require partners and suppliers to adhere to the Group’s security policies and contract terms, and cooperate fully in information security audits.

VII. Compliance

1. All personnel must adhere to this policy and applicable laws and regulations (including cybersecurity laws, trade secret laws, etc.).

2. Violations of this policy or related regulations shall be handled in accordance with company policies, and legal liability will be pursued based on the severity of the violation.
3. TCC Group employees must refrain from engaging in the following acts that infringe upon trade secrets:
   - Acquiring trade secrets through improper means or without authorization.
   - Obtaining, using, or disclosing trade secrets despite knowing, or negligently failing to recognize, that they constitute trade secrets.
   - Using or disclosing trade secrets after obtaining them, regardless of whether one knew or negligently failed to realize their nature as trade secrets.
   - Improperly using or disclosing trade secrets obtained through lawful means.
   - ailing to fulfill statutory duties to safeguard trade secrets or unjustly using or disclosing them.
4. The TCC Group's responsible managers, Information Security Department or dedicated teams, information asset owners and custodians, and project managers shall adopt heightened vigilance in safeguarding trade secrets. They will be presumed liable for any negligent actions associated with trade secret infringements unless evidence is provided to demonstrate the absence of fault.
5. TCC Group employees must familiarize themselves with legal requirements relevant to the company or their job responsibilities. Any violation of the law or internal regulations shall be subject to disciplinary actions in accordance with company policies and applicable legal provisions.

VIII. Employment Termination and Transfers

1. All employee transfers or contract terminations must adhere to company protocols.
2. During resignation or departmental transfers, employees shall complete all requisite handover and clearance procedures. Responsible department heads must periodically verify that all steps have been duly completed, ensuring the revocation of associated authorizations.
3. Access permissions to information assets shall be promptly adjusted to accommodate the employee's new role upon transfer.
4. Any act of infringement upon trade secrets shall constitute a severe breach of employment agreements and be addressed under both internal disciplinary measures and applicable trade secret laws.

IX. Review and Revision

This policy shall be reviewed at least annually and updated based on organizational strategies, technological trends, and stakeholder expectations, to ensure its ongoing relevancy and effectiveness. Procedures for policy revision or repeal shall adhere to the same processes governing its initial approval and adoption.

This policy shall take effect immediately upon formal approval and announcement. Subsequent amendments or repeals shall follow the same procedural standards.