TCC Group Information Security Policy

This Policy applies to all its subsidiaries in Taiwan, China and other jurisdictions, and other affiliates that are under the substantial control of the TCC Group, including all the employees of the TCC Group working in various offices around the world as well as any and all third-party suppliers, contractors, vendors and other business partners with access to the Group's internal information, to guide all relevant personnel in matters pertaining to information security, to facilitate the smooth operation of various business activities and to ensure that the TCC Group's information and systems are properly protected and secured.

I. Overview of Information Security Controls

The purpose of implementing information security controls is to ensure the security of the information used within the TCC Group. The term, "information", as used herein, refers to digital content and hard-copy documents created, collected, processed, utilized, transmitted, stored, and destroyed in the process of achieving the Group's operational objectives. The TCC Group's critical data and materials, such as correspondences, trade secrets, competitive intelligence, operating reports, core technologies, design drawings, key system codes, purchase orders, personnel data, financial information, and e-mails, are all part of the TCC Group's information and have significant value and impact on the Group's operations. Thus, during the life cycle of information, the TCC Group must ensure that critical information is secure and prevent any unauthorized disclosure, loss, alteration or destruction of such information from compromising the Group's operations, goodwill or capital. Therefore, ensuring the security of information within the TCC Group has become one of its top priorities nowadays.

II. TCC Group's Information Security Governance

In 2020, the TCC Group has established an organizational structure for information security and has since organized the Information Security Management Committee in accordance with ISO 27001 (Information Security Management System) to protect the confidentiality, integrity and availability of the Group's critical information systems and data, and to facilitate and audit the TCC Group's information security management system.

This information security organizational structure will encompass the Group's global deployment of information security measures and improve the information security management process. The top information security executive will head the Information Security Management Committee and report to the Company's board of directors periodically.

III. Information Security Objectives

1. Implementing appropriate safeguards and protective measures for the TCC Group's confidential and sensitive information to reduce the risk of information security incidents.

2. Mitigating the impact of information security incidents such as data destruction, theft, unauthorized disclosure, tampering, misuse, and infringement.

3. Continuously advancing the confidentiality, integrity and availability of the TCC Group's information security operations.

IV. Raising Employee Awareness on Information Security

Employees are the most important part of a corporation's information security operations. In order to raise the awareness of information security among the employees of the TCC Group, we offer regular information security training sessions every year to inform them of the basic information security concepts, the latest information security trends and the latest hacking techniques, and guide them to develop good information security work habits, such as conducting routine back-ups of work information, detecting abnormalities in incoming e-mails by carefully examining the e-mail addresses and domains, not clicking on unknown hyperlinks, being more cautious when accessing confidential and sensitive information or handling financial matters, and avoiding leaving excessive personal or company information on social media platforms, in order to reduce the probability of information security incidents.

V. Information Security Management Policy

1. Ensuring information security is the responsibility of each member of the TCC Group. In order to raise the awareness of information security, all the employees of the TCC Group must attend relevant training and education sessions from time to time, and learn about recent cases of information security incidents in Taiwan and other countries to strengthen their knowledge and awareness regarding information security so as to prevent social engineering attacks and information security incidents.

2. When engaging in business activities that involve the transmission of important information or sensitive data, appropriate information security measures must be put in place to reduce the risk of unauthorized disclosure of confidential and sensitive information.

3. Anti-virus software must be installed on personal computers used in the TCC Group's offices, and system and virus code updates must be performed regularly to reduce the risk of hacking and ransomware.

4. In the event of an information security incident, relevant authorities and units must be immediately informed in order to reduce any potential loss arising therefrom.

5. The Information Security Management Committee will conduct information security assessments or audits from time to time to review the soundness of the information security controls and weather the relevant management practices and procedures are in compliance with the relevant standards, laws and regulations, or information security requirements, and to provide recommendations for improvement to continuously increase the effectiveness of the TCC Group's information security management.

VI. This Information Security Policy is reviewed and revised at least once a year to keep up with the TCC Group's organizational and strategic development and the expectations of internal and external stakeholders and to ensure the effectiveness of this Information Security Policy.

VII. Compliance with this Policy and Relevant Laws

All personnel of the TCC Group shall comply with this Information Security Policy, and violators will be subject to applicable penalties under the relevant rules of the Company; where criminal or legal liabilities have arisen therefrom, such as under the applicable cyber security

laws, the Trade Secrets Act, the Copyright Act, and the Personal Data Protection Act, the TCC Group may take legal actions against such violators based on the severity of the circumstances.