啓碁科技資訊安全政策

- 所有關於資訊安全之規範皆應定期檢閱審核，以確保符合本公司訂定之資訊安全政策。
- 本公司內部所有正式員工、約聘員工、派遣人員、臨時僱員等公司所聘用之人員以及訪客及供應商，皆應清楚且遵循本公司所制定的資訊安全政策及相關規範。
- 本公司所有員工及外部單位人員，凡使用本公司資訊資產，均有責任及義務保護該資訊資產，以防止未經授權存取、篡改、破壞或不當揭露。所有資訊資產的存取與使用，應遵守本公司資訊安全相關規定。
- 員工有義務保護客戶商業機密暨智慧財產；嚴禁員工將客戶資訊揭露、告知與業務無關之同仁、廠商及其它客戶。
- 嚴禁所有人員於本公司資訊資產上安裝、使用、下載非法或未授權之軟體。
- 為確保本公司業務資訊之安全，本公司對於員工之工作職掌須作適當區隔，並僅授予完成工作所需之必要權限與必要資訊。
- 所有人員對於有發生安全事件、安全弱點及違反安全政策與程序之虞者，應隨時保持警戒，並應及時依程序進行通報。
- 本公司應依業務需求訂定業務持續運作計畫，相關同仁應參與定期測試演練以維持其適用性。
- 各部門應依文件重要性加以分級保護。
- 每年實施資訊安全相關訓練與宣導。
- 本公司響應永續政策，於採購使用之資訊設備時應優先考量具節能或綠色驗證標章之產品，並持續推動產品綠色設計、再生能源、參與減碳倡議、推動低碳轉型等策略。

WNC Information Security Policy

- The information security procedures shall be reviewed at regular intervals to ensure it is consistent with the information security policy.

- All employees, contractors, temporary workers, visitors, vendors, and other workers at the company shall understand and comply with the information security policy and relevant procedures.

- All employees of the company and external parties who use and access company IT assets have responsibilities and obligations to protect them against unauthorized access, modification, destruction, and improper disclosure. The use and access of IT assets shall proceed according to ISMS policy, procedures, and relevant regulations.

- Employees shall protect trade secrets and intellectual property. The disclosure of information about customers to non-relevant colleagues, vendors, and other clients is strictly prohibited.

- Installation, use, or downloading of illegal or unauthorized software on IT assets is forbidden.

- The company separates job duties and assigns access rights based on the principle of least privilege and a need-to-know basis to help ensure information security.

- All persons should be mindful of information security events, weaknesses, and suspected violations of the information policy and procedures. Immediately report information security events through the appropriate response and notification procedures.

- The company shall develop and implement Business Continuity Plans（BCP）in accordance with business needs which should be reviewed, tested, and drilled regularly to ensure they are up-to-date and effective.

- Information shall be classified in terms of its importance, sensitivity, and criticality.

- The company shall implement and promote an IT security awareness and training program for employees of the company annually.

- The company adheres to a sustainable policy and prioritizes the procurement and use of information equipment that is energy-efficient or carries green certification and committed to promoting green product design, renewable energy, participating in carbon reduction initiatives, and driving strategies for low-carbon transformation.