VSO ELECTRONICS CO., LTD.
Information Security Policy

(This English translation is prepared in accordance with the Chinese version and is for reference purposes only. If there are any inconsistencies between the Chinese version and this translation, the Chinese version shall prevail.)

Purpose:

To enhance the implementation of information security management at Hong Cheng Industrial Co., Ltd. (hereinafter referred to as "the Company") and ensure the confidentiality, integrity, and availability of business information. This is to comply with relevant laws and regulations, effectively reduce risks such as information asset theft, misuse, leakage, alteration, or destruction caused by human error, intentional acts, or natural disasters, and establish information security policies.

1. **Confidentiality:** Ensuring information is accessible only to authorized personnel.
2. **Integrity:** Ensuring information used is accurate and unaltered.
3. **Availability:** Ensuring authorized personnel can access required information.

Scope of Application:

This policy applies to all employees, outsourced service providers, and visitors to the Company.

Content:

1. All information security management regulations must comply with relevant government regulations, such as the guidelines for listed companies on information security controls and the Personal Data Protection Act.
2. Establish an information security organization, providing adequate human, material, and financial resources, and appoint dedicated personnel responsible for developing and promoting information security systems.
3. New employees are required to sign confidentiality agreements to ensure they understand the necessity of protecting confidential documents and raise awareness of information security.
4. Regular information security education and training are provided to employees, promoting security policies and ensuring sufficient security awareness.
5. All personnel are responsible for maintaining information security and complying with related management regulations.
6. An internal audit plan for information security management is established, with periodic inspections of personnel and equipment within the security management scope. Corrective and preventive measures are executed based on audit reports.

7. The information security policy should be evaluated and reviewed at least annually to ensure it aligns with current government regulations, business developments, and remains feasible and effective for operational continuity.
8. Prior to launching new systems and equipment, risk and security factors should be considered, and they must pass security checks to prevent compromising information security.
9. All information systems must be password-protected, and users should comply with security principles, including regular password changes. Computers should be locked or logged out when temporarily unattended or after work.
10. Physical and environmental security measures for the information room must be regularly inspected and maintained.
11. A disaster recovery management and backup drill plan should be implemented to ensure uninterrupted business operations.
12. A management mechanism for network and equipment usage is established, prohibiting employees from connecting unauthorized networks or devices to the Company's internal network.
13. The Company employs firewalls, intrusion detection, and antivirus software to protect internal networks from viruses and attacks. Security vulnerabilities are regularly assessed and patched to prevent system breaches.
14. Outsourced providers are evaluated for security risks related to commissioned work and are required to comply with security regulations.
15. Information security requirements for project management are clearly defined to ensure the confidentiality, integrity, and availability of project information, mitigating risks of sensitive information leakage and legal violations.
16. In the event of an information security incident, employees should promptly report to the IT department to prevent escalation and cooperate with relevant departments for resolution.