1. Information Security Risk Management Framework：

The responsibility unit for information security in this company is the Information Center, which consists of two personnel including the Information Manager and professional IT personnel. They are responsible for planning, implementing, and promoting information security management policies and awareness. The Audit Unit is responsible for monitoring and supervising information security. If any deficiencies are found during internal or external audits, the audited unit is required to submit relevant improvement plans and report them to the Board of Directors, and regularly track the effectiveness of the improvements to reduce internal information security risks.

2. Information Security Policy：

To implement information security management, the company has established an internal control system - computer information cycle and information security management policy. Through the joint efforts of all employees, the following policy objectives are expected to be achieved：

①Ensure the confidentiality, integrity, and availability of information assets.

②Ensure data access based on departmental authority and prevent unauthorized modification or use of data and systems.

③Ensure the sustainable operation of information systems.

④Prevent hacker attacks, various virus invasions, and improper and illegal use by humans.

⑤Regularly perform information security audit operations to ensure that information security is implemented and executed.

3. Specific Management Plan：

① The company's computer hosts, various application servers, and other equipment are placed in a dedicated machine room, which is controlled by access control and keeps records of entries and exits for inspection.

② The machine room management personnel should monitor the environment of the machine room, fill in the machine room log daily, and pay attention to the temperature, humidity, and operation of equipment such as air conditioning in the machine room.

③ The machine room hosts are equipped with uninterrupted power supply (UPS) equipment to avoid system crashes caused by sudden power outages or to ensure that temporary power outages do not interrupt the operation of computer application systems.

④ Establish a backup system that adopts daily incremental and weekly complete backup, and store it in a different location to reduce the risk and loss caused by system damage.

⑤ The entrance connecting to the outside is equipped with an enterprise-level firewall to block illegal intrusion by hackers.

⑥ Colleagues who access the company's internal network remotely must apply for relevant permissions before logging in and using it, and keep usage records for auditing purposes.

⑦ Colleagues who need remote access must apply for VPN encrypted secure channels to connect.

⑧ Regular education and promotion are provided to promote and strengthen internal colleagues' awareness of information security and enhance the company's overall information security level.

4. Resources allocated to information security management：

①Configuring enterprise-grade firewalls to block illegal intrusion attempts by hackers.

②Establishing a backup system with both hardware and software components, and regularly checking the availability of backup data to protect important company systems and data.

③Conducting daily system status checks, weekly regular backups, and storing backup media in off-site locations.

④Regularly promoting information security management policies to internal staff, and undergoing audits by accountants.

5. 預計投入

防毒軟體，包含郵件防毒、垃圾郵件過濾等，以避免惡意病毒程式之攻擊。

6. 執行狀況：

①本公司目前無重大資安事件導致營業損害之情事。

②續落實資訊安全管理政策目標，並定期實施復原計劃演練，保護公司重要系統與資料安全。