資通安全管理政策

為了使本公司ISMS（資訊安全管理系統）能切合實際需要，藉由維護本公司重要資訊系統的機密性、完整性與可用性，以支持業務之順遂，特頒布資通安全管理政策。本政策為高階指導原則，所有同仁、委外廠商皆有義務積極參與推動資通安全管理政策，以確保所有資訊系統安全維運，並期許所有人均能了解、實施與維持，以達資訊持續營運配合本公司業務遂行的目標。

1.落實資通安全，強化服務品質

貫徹執行ISMS，所有資訊作業相關措施，應確保資料之機密性、完整性及可用性，免於因相關資訊安全威脅遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度進行監控、審查及稽核資訊安全管理制度的工作，以完善的資通安全強化服務品質，提升服務水準。

2.加強資安訓練，符合法令要求規範

加強資安訓練，督導全體同仁落實資通安全管理，持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全相關法令要求之重要性，進而遵守法令及規定，藉此提高資通安全認知及能力，降低資通安全風險，達成資通安全管理法及個人資料保護法等相關法令要求事項。

3.規劃持續營運，迅速完成災害復原

訂定關鍵性業務核心資訊系統之緊急應變計畫及災害復原計畫，每兩年執行一次緊急應變流程演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，保持關鍵性核心資訊系統持續運作，達成本公司主要業務順利執行。

4.合理利用個資、防範個人資料外洩

對個人資料進行分類和評估，以確定保護的需求和措施。建立存取控制機制，於個資傳輸及共享方面採用加密與安全措施，定期評估委外廠商的遵守能力，並與委外廠商簽訂合約和協議以確保個資安全。強化員工教育訓練，增強個資保護意識。建立監控和審查機制，持續監視個資的使用、存取和傳輸，並及時檢測和應對異常活動或安全事件。確保不再需要時，個資能夠被安全且永久地刪除。

Information Security Management Policy

In order to ensure that the Company's ISMS (Information Security Management System) meets actual operational needs, and to support the smooth conduct of business by maintaining the confidentiality, integrity and availability of the Company's critical information systems, this Information Security Management Policy is hereby promulgated. This Policy constitutes a high-level guiding principle. All employees and outsourced contractors have an obligation to actively participate in and promote the Information Security Management Policy, so as to ensure the secure operation and maintenance of all information systems. All personnel are expected to understand, implement and maintain this Policy, thereby achieving continuity of information operations in support of the Company's business objectives.

1. Implement information security and enhance service quality

The ISMS shall be thoroughly enforced. All information operations and related measures shall ensure the confidentiality, integrity and availability of data, and shall protect data against risks of disclosure, damage or loss arising from information security threats. Appropriate protective measures shall be selected to reduce risk to an acceptable level, and the monitoring, review and audit of the information security management system shall be carried out, so that sound information security enhances service quality and raises service standards.

2. Strengthen information security training and comply with statutory and regulatory requirements

Information security training shall be strengthened and all employees shall be supervised in implementing information security management. Appropriate information security education and training shall be conducted on an ongoing basis to establish the concept that "information security is everyone's responsibility", so that employees understand the importance of information security related legal requirements and duly comply with applicable laws and regulations. This raises information security awareness and capability, reduces information security risk, and fulfils the requirements of the Cyber Security Management Act, the Personal Data Protection Act and other relevant laws and regulations.

3. Plan for business continuity and achieve rapid disaster recovery

Emergency response plans and disaster recovery plans shall be established for the core information systems supporting critical business operations, and an emergency response drill shall be conducted once every two years. This ensures that, in the event of information system failure or a major disaster, rapid recovery can be achieved and critical core information systems can be kept in continuous operation, so that the Company's principal business activities proceed without interruption.

4. Use personal data reasonably and prevent personal data breaches

Personal data shall be classified and assessed in order to determine protection requirements and measures. Access control mechanisms shall be established, and encryption and security measures shall be adopted for the transmission and sharing of personal data. The compliance capability of outsourced contractors shall be evaluated periodically, and contracts and agreements shall be signed with such contractors to ensure the security of personal data. Employee education and training shall be strengthened to raise awareness of personal data protection. Monitoring and review mechanisms shall be established to continuously monitor the use, access and transmission of personal data, and to detect and respond to abnormal activities or security incidents in a timely manner. It shall be ensured that personal data can be securely and permanently deleted when it is no longer required.