目　　錄

1. 目的 Purpose：

制訂本《資訊安全管理手冊》對資訊安全管理制度之範圍、管理政策、流程、規範、辦法、要求及角色與權責，做為資訊安全管理制度活動之作業準則，以確保資訊安全管理制度之實施，能符合管理需要與相關國際標準要求。

Formulate this "Information Security Management Manual" on the scope of the information security management system, management policies, processes, specifications, methods, requirements, roles and responsibilities, as the operating guidelines for the activities of the information security management system, to ensure implementation of the information security management system comforms to the management needs and the requirements of relevant international standards.

2. 範圍 Scope：

2.1. 管理制度 Management system

根據公司管理需要，參考 ISO/IEC 27001:2022 國際標準要求之規定製定，以滿足 ISO/IEC 27001:2022 國際標準認證之要求。

According to the company's management needs, it is formulated with reference to the requirements of the ISO/IEC 27001:2022 international standard to meet the requirements of the ISO/IEC 27001:2022 international standard certification.

2.2. 組織範圍 Organizational Scope

本文件適用於公司各部門。

This document is applicable to all departments of the company.

3. 名詞定義 Definition of terms

本手冊中所使用名詞，請參考「**名詞解釋**」之說明。

For the terms used in this manual, please refer to the explanation in "Terms Explanation".

4. 政策與目標 Policies and Objectives

4.1. 資訊安全政策 Information Security Policy

由總經理指派資訊安全長(以下簡稱 資訊長)成立資訊安全委員會，負責擬定資訊安全政策。資訊安全政策於本公司資訊長審查核可後，發佈實施；包含資訊安全管理政策和資訊安全防護措施政策二個部分，應每年定期進行審查與維護，說明如下：

The chief information security officer (hereinafter referred to as the CIO) is appointed by the general manager to establish an information security committee, which is responsible for formulating information security policies. The information security policy shall be released and implemented after the review and approval of the CIO of the company; it includes two parts, the information security management policy and the information security protection measures policy, which shall be regularly reviewed and maintained every year, as explained below:

4.1.1. 資訊安全管理政策(Information Security Management Policy)

4.1.1.1. 資訊長應確保建立資訊安全政策和目標，且與本公司之營運策略方向相容。

The CIO shall ensure that information security policies and objectives are established and are compatible with the company's business strategy.

4.1.1.2. 本公司之資訊安全管理政策為「提供安全與持續運作之資訊系統維護、測試與維運環境，確保資訊系統及資訊之安全，達成本公司資訊安全管理目標。」

The company's information security management policy is "to provide a safe and continuous operation of the information system maintenance, testing and execution environment, to ensure the security of the information system and information, and to achieve the company's information security management goals."

4.1.1.3. 資訊安全管理政策之發佈更新，應讓本公司同仁知悉，並依據需求，讓關注方了解政策之要求。

4.1.2. 資訊安全防護措施政策 Information Security Protection Measure Policy

4.1.2.1. 移動裝置管理政策 Mobile Device Management Policy

所有界接到公司網路與作業環境之移動裝置，應經網路管理員與權責主管審查核准，包括手機、筆記型電腦、平版電腦、或其他具有儲存和連線功能之移動式裝置，始可使用。

All mobile devices connected to the company's network and working environment can be used after being reviewed and approved by the network administrator and the supervisor in charge, including mobile phones, notebooks, tablets, or other mobile devices with storage and connection functions.

4.1.2.2. 遠距工作管理政策 Telework Management Policy

經由外部網路連接公司網路與作業環境之遠距工作，應經網路管理員與權責主管審查核准，且作業之資訊設備應具備公司同意之保護機制。

The remote work connected to the company's network and the working environment through an external network should be reviewed and approved by the network administrator and the supervisor in charge, and the information equipment used for the operation should have a protection mechanism approved by the company.

4.1.2.3. 存取管制政策 Access Control Policy

資訊系統與資訊之存取管制包含實體與邏輯二部分。界接公司之資訊資產設備，不得設於公司外部無人看管或未具有保護機制之位置。具有存取資訊系統或網路設施之資訊設備，必須要具有唯一識別機制，且使用者僅能存取和其工作相關之資訊系統與資訊，對於使用者之存取應能記錄存取軌跡。擁有特別存取權限之使用者，應限制存取權限之配置與使用。

Information system and information access control include physical and logical parts. The information asset equipment connected to the company shall not be located outside the company where it is unattended or has no protection mechanism. Information equipment with access to information systems or network facilities must have a unique identification mechanism, and users can only access information systems and information related to their work, and access traces should be recorded for user access. Users with special access rights should restrict the configuration and use of access rights.

4.1.2.4. 加密管理政策 Encryption Management Policy

機密等級為「機密」之資訊，於進行傳輸或儲存時，皆應加密保護。

Information classified as "Confidential" shall be encrypted for protection during transmission or saving.

4.1.2.5. 金鑰管理政策 Key Management Policy

公司使用之金鑰，每年應定期審查金鑰的有效性，金鑰生命週期之管理，應由專人管理。

For the keys used by the company, the validity of the keys should be reviewed regularly every year, and the management of the life cycle of the keys should be managed by specialist.

4.1.2.6. 螢幕保護與桌面淨空政策 Screensaver and Desktop Clearance Policy

4.1.2.6.1 本公司所有資訊設備，包括伺服器、個人電腦、筆記型電腦和具有操作畫面之移動裝置，應設定電腦螢幕保

護時間，電腦在無人操作情況下，最長不得超過 15 分鐘，系統畫面應自動進入密碼保護狀態。
All the company's information equipment, including servers, personal computers, notebooks and mobile devices with operation screens, should set the computer screen protection timeout. When the computer is unmanned, the longest timeout shall not exceed 15 minutes. The screen should automatically enter the password-protected state.

4.1.2.6.2 人員桌面不應存放機密等級為「限閱」及「機密」之資訊。人員離開座位時，應將桌面整理淨空，機密等級為「限閱」及「機密」之資訊，應採取保護措施。
Personnel desktops should not store information classified as "restricted" and "confidential". When personnel leave their seats, the desktop should be tidied up, and information with a confidentiality level of "restricted" and "confidential" should be protected.

4.1.2.7. 備份政策 Backup Policy
資訊系統與資訊應依其可用性要求，擬定備份計畫，並依據計畫進行備份作業、保存及還原測試。
The information system and information shall draw up a backup plan according to their usability requirements, and conduct backup operations, save and restore tests according to the plan.

4.1.2.8. 資訊移轉管理政策 Information Transfer Management Policy
在公司內部移轉之資訊，若機密等級為「機密」應設定保護機制。公司與外部團體間之資訊移轉，應事前申請並經資訊保有之權責單位主管核准後，方能移轉。與外部團體間如為移轉機密等級為「機密」之資訊，移轉過程應有安全之保護機制。
For information transferred within the company, if the confidentiality level is "confidential", a protection mechanism should be set up. The transfer of information between the company and external groups shall be subject to prior application and approval by the supervisor of the responsible unit responsible for information retention. If information with a confidentiality level of "confidential" is to be transferred with an external party, a security protection mechanism should be in place during the transfer process.

4.1.2.9. 安全開發政策 Secure Development Policy
依據資訊系統安全設計、開發、測試、發行與維護之作業準則，進行資訊系統之安全設計、開發、測試、發行與維護作

業。

Carry out security design, development, testing, release and maintenance of information systems in accordance with the operational guidelines for information system security design, development, testing, release and maintenance.

4.1.2.10. 委外廠商資訊安全管理政策 Information Security Management Policies of Subcontractors

權責單位應與委外廠商建立專案之資訊安全管理需求，並在委外廠商履行合約義務過程中，實施必要之管理與稽核活動，確保委外廠商提供之服務與產品，符合專案之資訊安全管理需求。

The responsible unit should establish the information security management requirements of the project with the outsourced manufacturer, and implement necessary management and audit activities during the process of the outsourced manufacturer's performance of contractual obligations to ensure that the services and products provided by the outsourced manufacturer comply with the information security of the project managment needs.

4.2. 資訊安全管理目標 Objectives of information security management

4.2.1. 本公司之資訊安全管理目標為「在合於法令、法規與合約要求條件下，確保資訊資產的機密性、完整性與可用性，提供持續可用之資訊服務。」

The company's information security management goal is to "ensure the confidentiality, integrity and availability of information assets and provide continuously available information services under the conditions of compliance with laws, regulations and contract requirements.

4.2.2. 為達成資訊安全管理目標，應參考 ISO/IEC 27001 國際標準要求，建立資訊安全管理制度，對資訊安全管理制度實施範圍內之資訊資產採取適當保護措施，以維持資訊資產之機密性、完整性與可用性，提供客戶安全之資訊服務並滿足其需求。

In order to achieve the goal of information security management, an information security management system should be established with reference to the requirements of the ISO/IEC 27001 international standard, and appropriate protection measures should be taken for the information assets within the implementation scope of the information security management system to maintain the confidentiality, integrity and availability of information assets, provide customers with secure information services and meet their needs.

4.2.3. 為確保資訊安全管理制度之實施，能夠達成營運需要，各項作業流程應根據資訊安全管理目標，訂定作業流程目標。

In order to ensure that the implementation of the information security management system can meet the operational needs, each operation process should set the operation process objectives according to the information security management objectives.

4.2.4. 資訊安全管理目標之評估與檢視 Evaluation and inspection of information security management objectives
資訊安全工作小組應每年檢視與評估資訊安全管理目標，提出修訂建議，提請資訊安全委員會審查核准。
The information security working group shall review and evaluate the information security management objectives every year, propose revision recommendation and submit them to the information security committee for review and approval.

5. 資訊安全管理制度制訂與實施 Formulation and implementation of information security management system

5.1. 資訊安全工作小組應每年或當發生重大變更時進行資訊安全組織全景分析作業，分析結果應記錄「**資訊安全組織全景分析表**」中。並依據資訊安全全景分析結果與資訊安全管理政策與目標之要求，制訂與維護資訊安全管理制度、推動與管理資訊安全管理制度之實施、監控與評估資訊安全管理制度實施績效、持續改善資訊安全管理制度。
The information security working group should carry out an information security organization panorama analysis every year, and the analysis results should be recorded in the "Information Security Organization Panorama Analysis Form". And according to the results of information security panorama analysis and the requirements of information security management policies and objectives, formulate and maintain information security management system, promote and manage the implementation of information security management system, monitor and evaluate the implementation performance of information security management system, and continuously improve information security management system.

5.2. 資訊安全管理制度要求係以滿足資訊安全組織全景分析與資訊安全風險評鑑之結果所訂定，資訊安全工作小組應遵循相關政策及作業規定，督導各部門依規定實施各項作業流程要求。
The requirements of the information security management system are formulated to meet the results of Information Security Organization Panorama Analysis and the information security risk assessment. The information security working group should follow the relevant policies and operating regulations, and supervise all departments to implement various operating process requirements in accordance with the regulations.

6. 審查與修訂「適用性聲明書」Review and revision of the "Applicability Statement"

資訊安全工作小組應根據公司營運與 ISO/IEC 27001 要求，每年審查與修訂資訊安全控制措施之「**資訊安全管理系統適用性聲明書**」，並提請資訊安全委員會審查核准。
The information security working group should review and revise the "Statement of Applicability of Information Security Management System" of

information security control measures every year according to the company's operation and ISO/IEC 27001 requirements, and submit it to the Information Security Committee for review and approval.