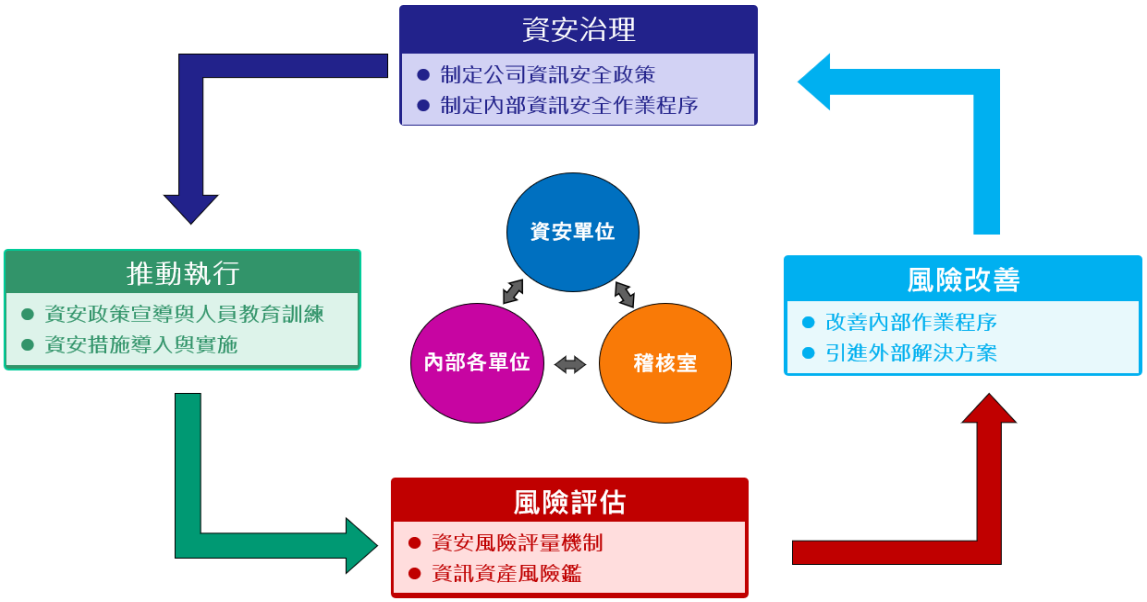
資訊安全管理政策

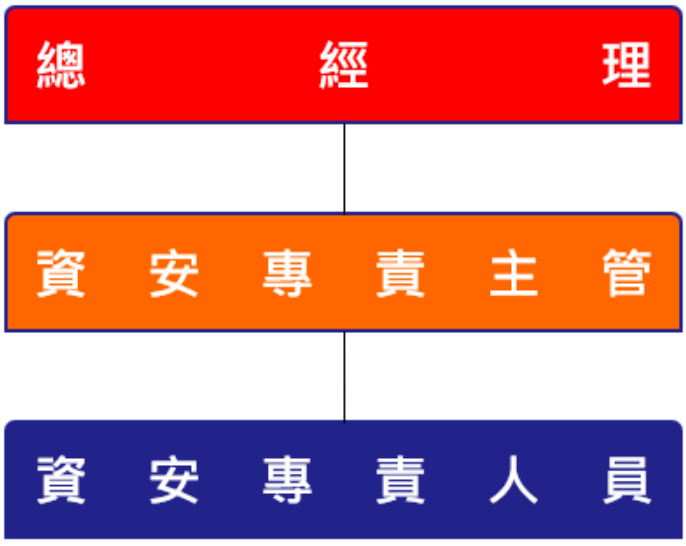
公布日期：2022 年 1 月 5 日

版本：2.1

資訊安全組織架構

本公司設立資訊安全組織架構，由總經理擔任總召集人，資訊安全長則由資訊主管擔任；資訊安全稽核小組，則由稽核室同仁擔任。資訊安全委員會之委員由各單位主管擔任，資訊安全執行小組以及緊急處理小組，則由資訊部同仁擔任。資訊安全組織將不定期召開管理審查會議，制訂與檢討資訊安全管理目標及政策，並透過資訊安全組織，以推動資訊安全管理審查會議決議之資訊安全作業，促使資訊安全管理系統能深入持續穩健運作。





前言

為有效管理資訊使用上的安全，特訂立資訊安全辦法，作為相關資訊使用網路安全、設備安全及軟體應用安全的管理辦法，本辦法共分三個章節，依性質及管理目的分為「網路安全」、「電腦設備安全」及「應用軟體安全」。

共同規範

1 名詞解釋與縮寫符號：描述在各文件中所使用到的特殊名詞、縮寫符號與簡稱。定義用字需解釋清楚、縮寫符號則需說明全文及其意義，並以英文字母順序表列。

2 參考文件資料：參考資料項目為一般國際標準文件所必需，記載並說明各文件中所參考引用之文獻及範例，軟體專案之文件，組織及作業手冊之編號、標題、改訂版、與日期，及其他相關的文件等。

第一章：網路安全

1 文件目的：為使本公司各級單位充分有效使用網路資源，特訂立此管理辦法。

2 工作說明：

2.1 電腦網路使用與資訊安全管理：

2.1.1 電腦網路使用以網域帳號及密碼控管。

2.1.2 禁止將帳號與密碼交付他人運用，並不得使用他人帳號與密碼登入電腦，離職時由資訊單位將密碼帳號刪除。

2.1.3 禁止利用點對點軟體分享下載資料或將公司內電腦資料匣開放讓外部人員分享使用。

2.1.4 網路使用者應關閉網路資源分享功能，防止資料外流，並不得以任何手段蓄意干擾或妨害網路系統正常運作。

2.1.5 禁止利用網路散播病毒、發表毀謗言論、傳送色情圖片等不當行為。

2.1.6 網路使用者應尊重智慧財產權，使用者避免下列可能涉及侵害智慧財產權之行為：

2.1.6.1 來路不明或未經授權之電腦程式。

2.1.6.2 下載、拷貝受著作權法保護之著作。

2.1.6.3 未經著作權人同意,將受保護著作資料上傳於外部公開網站或部落格中。

2.1.6.4 BBS或其他線上討論區上之文章，經作者明示禁止轉載，而仍然任意轉載或轉寄。

2.1.7 廠商進行維護時應採行必要的事前預防及保護措施，以預防及偵測電腦病毒、木馬及邏輯炸彈等惡意軟體之侵入。

2.2 電子郵件安全管理：

2.2.1 郵件軟體應關閉信件預覽功能。

2.2.2 來路不明電子郵件不宜任意開啟，以免啟動駭客惡意執行檔。

2.2.3 敏感性或具保密需求之郵件，應採取適當加密措施。

2.2.4 禁止以匿名信或偽造他人名義發送電子郵件。

第二章：電腦設備安全

1 文件目的：為使本公司各級單位充分有效使用及管理電腦設備，特訂立此管理辦法。

2 工作說明：

2.1 伺服器主機安全管理：

2.1.1 電腦伺服器主機設備應妥善保管，並以帳號密碼控管。

2.1.2 伺服器主機除由系統維護人員基於業務需要執行啟動及操控外，其他人員不得擅自操作。

2.1.3 電腦伺服器專用電源插座，不得使用於電腦以外之設備，以免耗用不斷電系統電源，造成跳電當機，影響電腦正常運作。

2.1.4 電腦伺服器周圍環境不得攜入或存放磁性、放射性、易燃性及易爆性物品，並嚴禁嬉戲、吸菸及飲用食物。

2.2 個人電腦設備安全管理：

2.2.1 電腦應使用專用電源延長線，避免與其他電器用品共用插座，以免電力無法負荷導致火災等危害安全情事。

2.2.2 個人電腦設備應維持整潔，電腦風扇出口禁止雜物阻擋，並注意通風，以維安全。

2.2.3 使用個人電腦設備應盡善良保管人維護責任，禁止任意拆卸或安裝硬體。

2.2.4 個人電腦於下班或公出時應關機以維設備安全。

2.3 電腦設備作業系統安全管理：

2.3.1 電腦設備作業系統及相關伺服器軟體應適時更新軟體及進行漏洞修補。

2.3.2 電腦設備作業系統應安裝防毒軟體並適時更新病毒資料庫。

2.4 個人資訊安全管理：

2.4.1 敏感性或具保密需求之資料應採檔案加密，存放辦公室固定電腦為主，並注意實體隔離，勿存放於隨身儲存設備中。

2.4.2 若需公務電腦資料攜回家中處理，應先將隨身儲存設備中之敏感性或具保密需求資料刪除，以維安全。

2.4.3 同仁經由網際網路下載檔案或使用隨身碟(USB)應立即進行病毒掃描，確認安全無毒後才可使用。

第三章：應用軟體安全

1 文件目的：本措施在於管理本公司應用軟體安全，並做有效應用與管理。

2 工作說明：

2.1 軟體購置與使用，應採合法授權軟體，同時符合智慧財產權相關法規規定。

2.2 一般性應用軟體採購可依需求提出申請，並由資訊單位彙整，經核定後依採購程序辦理，購置後統一由資訊單位納入管理。

2.3 購入之軟體應配合總務財產管理人員統一列冊管理，有關授權證明、原版程式及使用手冊由資訊單位妥善儲存與管理。

2.4 列冊管理之軟體依需要提供各單位使用，並應登錄使用者單位、姓名及使用日期等相關資料供管理參考。

2.5 採購應用軟體與系統、資料庫及程式開發等應用程式，應注意所有輸入欄位應有字元檢查功能，排除不必要特殊字元，以防止資料庫隱碼（SQL-Injection）攻擊。

第四章：資訊安全保險

1 文件目的：為使本公司從資安策略、應變機制、軟硬建設等技術面，掌握資安風險的曝險程度，將委請專業保險經紀公司評估比對風險與轉嫁程度、並審核理賠鑑識機構資質與確認理賠實務，以確保集團資安風險得到最佳的保險保障，將在研究完成後立即安排保險保障。本措施在於投保資安保險之前，須執行之具體基本防護。

2 工作說明：

2.1 指定一位資訊安全人員負責執行資訊安全工作，且每年定期參加十五小時以上資訊安全專業課程訓練。

2.2 每年辦理二次員工資訊安全宣導。

2.3 網路系統安全評估：

(a) 定期評估網路系統安全（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等）。
(b) 定期修補網路設備之安全漏洞。

2.4 電腦病毒及惡意軟體之防範：

(a)安裝防毒軟體，並及時更新程式及病毒碼。
(b)定期對電腦系統進行病毒掃瞄

2.5 每半年辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，評估其相關風險或安裝修補程式。

2.6 提高風險控管能力，訂定相關辦法規範資料復原作業以及系統備援作業程序等。

2.3 逐步執行多項資安演練：例如核心資訊系統居家辦公演練、病毒爆發演練、社交工程演練、資訊系統異地備援演練等。

本規範自發布日實施。