資通安全風險管理

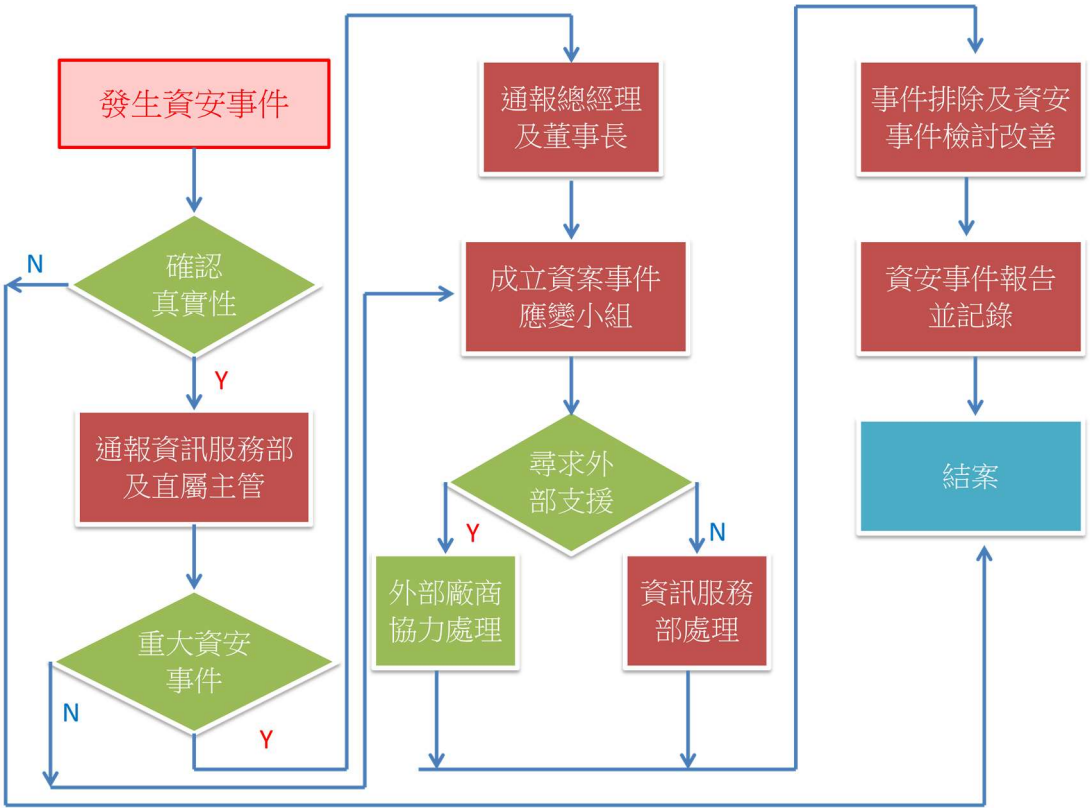
為保護本公司營業秘密、智慧財產及公司機密資訊，降低公司營運風險，並對個人資料之保護與管理，本公司已訂定各項電腦化資訊系統處理作業及個人資料保護等相關管理辦法，以落實內控制度與維護資訊安全政策。透過每年檢視和評估其安全規章及程序，確保其適當性和有效性。以下分項進行詳細說明：

(1)資通安全管理架構

本公司資訊安全之權責單位為資訊服務部，並設有資安專責主管及資安專責人員各一名，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全觀念，稽核室為資訊安全監理之查核單位，內部訂定各項資訊相關內部作業規定及個人資料保護管理辦法，定期進行相關資安檢測，持續改善各項作業，提升公司資訊安全。

本公司注重資訊安全事項，必要時定期向經理人會報資安管理運作情形。

本公司訂有資訊安全事件通報程序，資安事故之通報及處理，皆遵行處理。



(2)資通安全政策

A. 確保本公司資料、系統、設備及網路通訊安全，積極的阻絕外界之入侵、破壞，消極的確保本公司資料、系統、設備可被破壞還原。

B. 確保系統資訊帳戶存取權限與系統之變更均經過公司規定程序授權處理，限縮特權帳戶之使用，區分特權帳戶使用之範圍。

C. 落實銷毀程序，已報廢之電腦儲存媒體應加以銷毀避免資料意外暴露外流。

D. 監控資訊系統之安全狀態與活動紀錄，有效掌握並處理資訊安全事件。

E. 維護資料與系統之可用性與完整性，發生災害或受破壞時，可回復正常作業。

F. 建立員工資訊安全觀念，落實各項資訊作業執行。

G. 本公司內部稽核計劃項目包含資通安全檢查，透過稽核單位查核，加強內控管理。

(3)具體管理方案及投入資通安全管理之資源

本公司之內部系統皆處於虛擬網路之中，外部網路受隔離無法直接進入，並已採用多重網路安全防禦系統，位於網路前端之防火牆、郵件內容安全控管系統負責過濾網路進出連線的內容，能防禦外部網路攻擊，並即時封鎖最新惡意軟體、有害之網站連結、垃圾電子郵件等威脅。

位於內部之主機及端點皆由中控台佈署防毒軟體，落實防毒端點安裝、提升部署涵蓋率，隨時更新病毒碼與即時辨識惡意行為特徵，能即時攔截病毒木馬蠕蟲、勒索軟體、文件夾帶之惡意程式等，有效降低被駭客攻擊損害之風險。

具體管理方案及資源：

A. 系統帳號生命週期管理與權限帳號管理

依各業務範圍、權責分別設定使用者之帳號及權限，資料之存取皆需透過簽核流程經各權責主管申請並核准後始能使用與變更。使用者一旦離開原職務，立即撤銷該使用者之帳號及權限，以防範未經授權之使用。

B. 資料存取紀錄稽核備存

能紀錄系統檔案文件存取之軌跡記錄、往來郵件等資料，進行歸檔保存。報廢程序完成之電腦均執行硬碟拆解破壞以符合法規遵循的管理制度及資安政策。

C. 安全防護措施

藉由各項防毒軟體、網路防火牆、郵件過濾機制、機敏性資料處理及文件加密、定期檢測安全性漏洞修補，各項軟體及通訊軟體

安裝管控，以IPS阻隔網段或主機之間的弱點攻擊，保障公司各項業務的資訊安全。

本公司已加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)組織，可事先取得資安預警情資、瞭解資安威脅與弱點資訊及通報資通安全事件，共同維護台灣網路安全，提升台灣整體資安防護能量。

D. 管理安全性評信

定訂服務主機連線來源的合理性，登入的帳號是否存在濫用或誤用情形，有無未知服務正在運作，監控並限縮VPN連線，限制遠端軟體使用。

E. 資訊系統持續運作

訂定備份機制及備援計畫，重要系統與文件皆採取每日、每週及每月之本地備份，相關之備份資料以磁帶方式存放到異地資料中心(IDC)做為異地備份。並每年定期執行系統資料災害還原測試演練，以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為災害造成之資料損失風險。

F. 教育訓練

新進人員教育訓練中加入資安課程項目，並不定期辦理資訊安全教育訓練及宣導,建立員工資訊安全認知及尊重智慧財產權概念，保護人員及公司資訊。

本公司112年度辦理資訊教育訓練課程，建立同仁觀念。

項目	課程數	總人次	總人時
1. 資訊安全教育宣導	2	77	77
2. 資安宣導-電子郵件安全與社交工程防範	2	56	56
3. 資安宣導-勒索軟體介紹與防護	2	51	51

本公司資通安全管理之相關事項定期提報董事會，
112 年提報日期為 112 年 1 月 12 日，
最近一次提報日期為 113 年 1 月 19 日。

本公司資訊部門執行作業依規定程序均能落實執行,風險評估結果尚屬良好，近來資安攻擊事件頻傳，本公司積極加強資訊安全維護措施，建立員工資安觀念，降低公司營運風險。最近年度並無因重大資通安全事件之情形。