資安風險評估分析及其因應措施等重要風險評估之事項：

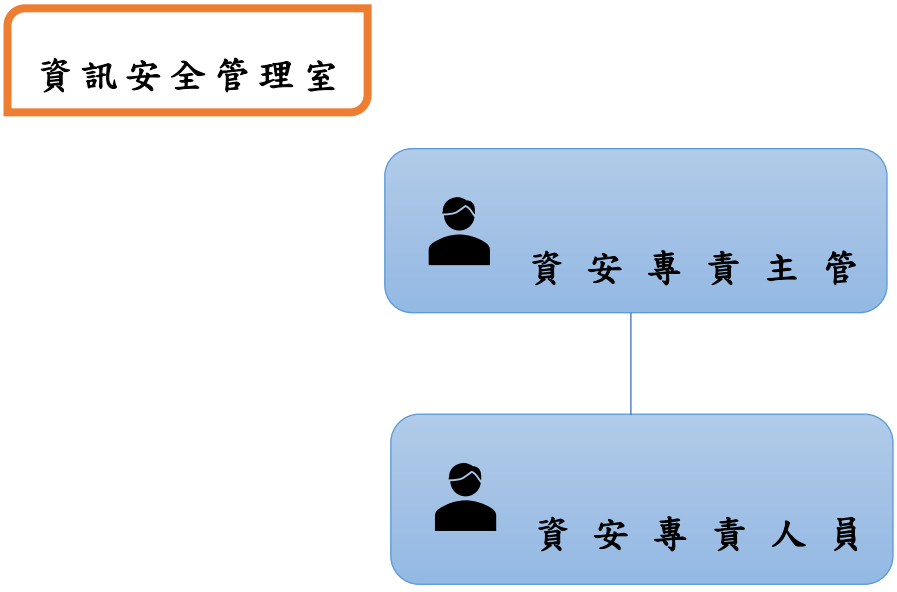
1. 資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源:

(1)資訊安全管理架構

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全管理室，為資安專責單位，包含資安專責主管及至少一名以上的資安專責人員，負責資通安全事務的規劃與執行。其中，資通安全風險管理架構至少每年一次於董事會中報告重大議題或規劃。

(2)資訊安全風險管理機制

執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理。



(2)資訊安全政策

本公司訂定「資訊設施管制作業程序」及「資通安全作業程序」於經董事長核准以作為本公司資訊安全管理之最高指導原則；訂定本公司資訊作業標準，發揮企業電腦化最大效能，提供各單位最即時資訊，服務公司所有電腦使用者，增進工作效率。

- **資訊安全之政策願景：**

(1)強化人員認知。
(2)避免資料外洩。
(3)落實日常維運。
(4)確保服務可用。

- **資訊安全之目標：**

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。
(1)辦理資通安全教育訓練，推廣員工資通安全之意識與強化其對相關責任之認知。
(2)保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
(3)使用合法授權軟體並定期進行內部與外部稽核，確保相關作業皆能確實落實。
(4)確保本公司關鍵核心系統維持一定水準的系統可用性。

- **資訊安全之範圍：**

(1)人員管理及資訊安全教育訓練。
(2)電腦系統安全管理。
(3)網路安全管理。
(4)系統存取管制。
(5)系統發展及維護安全管理。
(6)資訊資產安全管理。
(7)實體及環境安全管理。
(8)資訊系統永續運作計畫管理。
(9)資訊安全稽核。

並宣導下列資訊安全政策：

(1)員工資安意識加強：將具風險的資安威脅訊息資及應對方式不定期與公司員工宣導，避免員工不經意間落入資安威脅的陷阱，加強員工資安意識。

(2)網路攻擊、病毒威脅：網路防火牆建立多層次的防禦及檢測，終端電腦安裝防毒軟體，並統一進行監控及防護，降低網路威脅入侵及全面掌握資安狀態。

(3)確保資訊服務不中斷：針對重要營運服務及資料，均有作本地及異地備份及還原演練，如遇無法避免主營運系統或資料庫毀損或運行中斷時，確保符合預期資訊系統復原時間。

(4)營業機密文件保護：針對營業核心研發文件，均採取獨立資料庫系統並且檔案加密管理方式，保障公司競爭優勢不被輕易獲取。

- **資訊安全的原則及標準：**

(1)定期宣導資訊安全教育，包括資訊安全政策、資訊安全法令規定、 資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊 安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。

(2)為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

(3)為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

- **員工應遵守之相關規定：**

(2)電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，以維護資料完整性。

(3)禁止使用無版權軟體。

(4)進入主機後，若作業結束或長時間不使用機器時，應退出機器，以免資料機密外洩，為別人所破壞或造成當機之困擾。

(5)電腦設備之擺放位置除以方便為原則外 ，應遠離茶水、咖啡、日曬或潮溼地點，以延長其壽命。

(6)離職或新舊職務交接時，由資訊單位衡量資料相關性作適當處置。

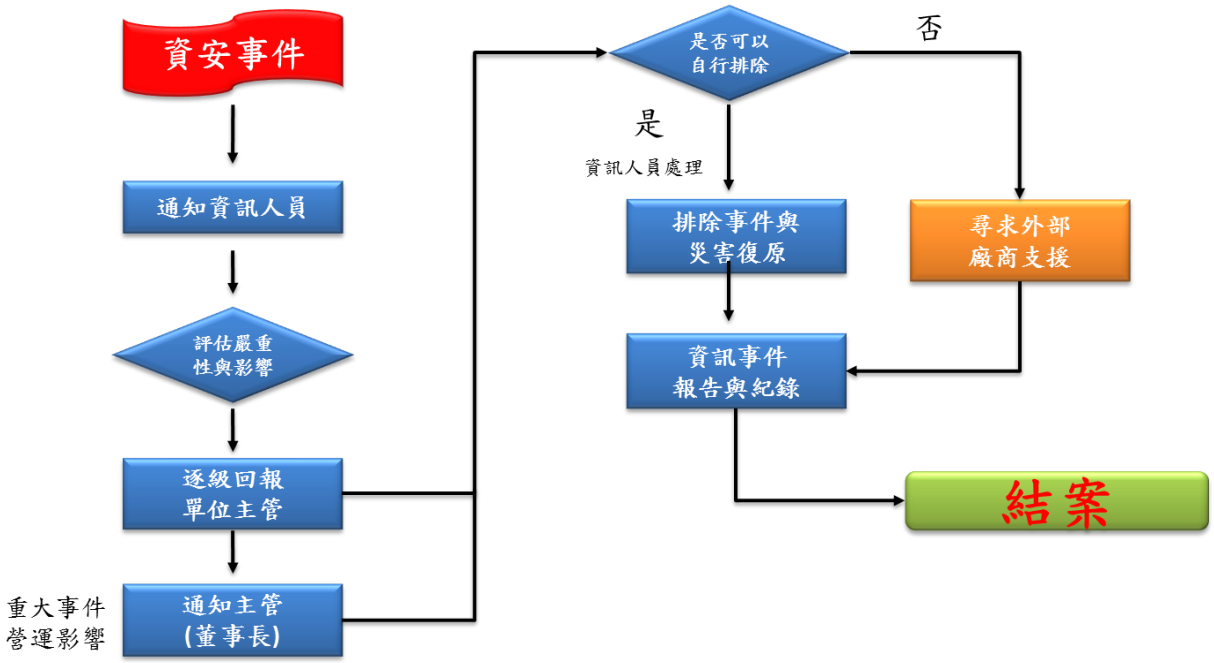
(7)電腦設備無法正常作業時，使用者應立即通知資訊單位，以便檢查或維修。

運作情形

本公司自 2008 年起積極推動落實資訊安全政策，主要運作情形如下:

- 2008 年頒布本公司「資訊設施管制作業程序」。
- 2022 年本公司的資訊安全所採行的控制措施與運作情形已於 2022 年 11 月 04 日委由財會經理彙整相關資訊安全執行成果並於董事會中報告。
- 2023 年訂定本公司「資通安全作業程序」。
- 2023 年本公司的資訊安全所採行的控制措施與運作情形已於 2023 年 10 月 31 日委由財會經理彙整相關資訊安全執行成果並於董事會中報告。
- 2024 年本公司的資訊安全所採行的控制措施與運作情形已於 2024 年 10 月 24 日委由財會經理彙整相關資訊安全執行成果並於董事會中報告。

(3)資安事件處置措施


資安事件
通知資訊人員
評估嚴重性與影響
逐級回報單位主管
重大事件營運影響
通知主管(董事長)
是否可以自行排除
否
是
資訊人員處理
排除事件與災害復原
尋求外部廠商支援
資訊事件報告與紀錄
結案

(4)具體管理方案及投入資通安全管理之資源

- **資通安全具體管理方案**

項目	具體管理措施
防火牆防護	• 防火牆設定連線規則。
使用者上網控管機制	• 使用自動網站防護系統控管使用者上網行為。 • 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	• 使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	• 作業系統自動更新，因故未更新者，由資訊人員協助更新。
郵件安全管控	• 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 • 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
資料備份機制	• 重要資訊系統資料庫皆設定每日備份。
重要檔案上傳伺服器	• 公司內各部門重要檔案存放於伺服器，由資訊部統一備份保存。
資安險	• 本公司客戶主要為企業客戶，無消費者個資保管風險，於評估市面資安險種保險範圍、適用行業等項目後，暫不投保資安險，但因應資訊安全所面臨的挑戰，已導入相關軟硬體，例如防火牆、防毒、入侵防護系統…等，並持續關注資訊環境變化趨勢，並強化公司同仁資安危機意識及資安處理人員應變能力。

• 投入資通安全管理之資源

針對系統主機的作業系統或重要軟體升級、災害復原演練等重要的資安工作，資安管理室每月皆會定期檢討規劃與執行進度，並透過不定期的社交工程演練、資安健檢服務等，判斷使用者的資訊安全觀念是否足夠、資訊設備資源投入與系統配置是否存在漏洞，編列資安預算後執行。

• 資訊安全的管理措施