【資訊安全對象與範圍】

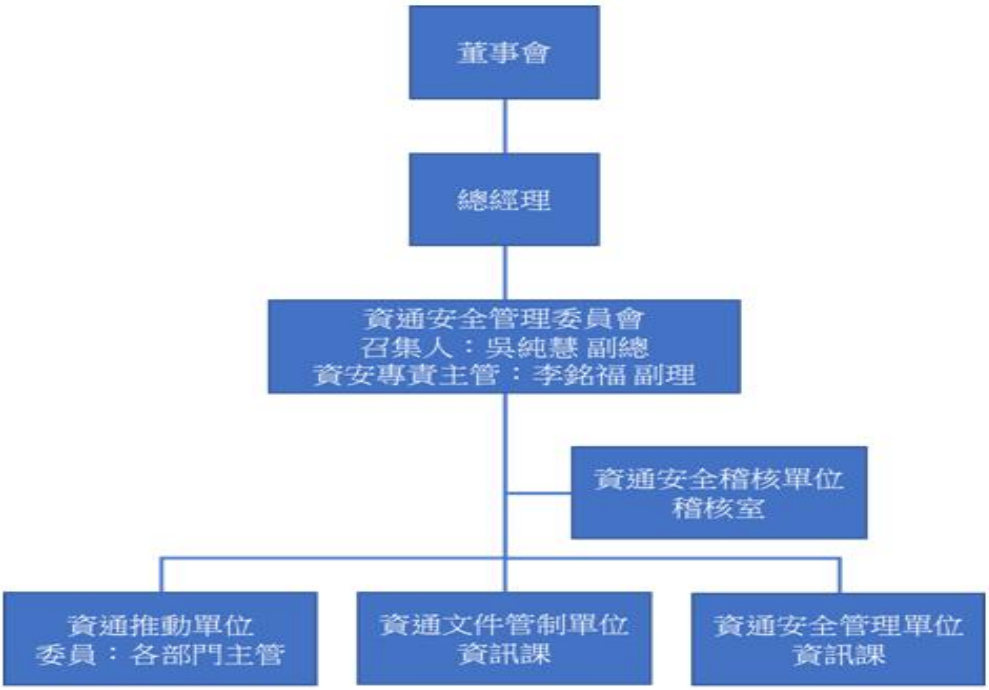
對象：包括員工、客戶、供應商和股東以及營運相關資訊軟硬體設備。

範圍：適用為資訊機房維運、業務持續運作系統及網站系統維護之安全管理，已充份掌握資訊運作及管理過程並滿足各項安全要求與期盼，主要類別如下：

(1) 資訊記錄
(2) 電腦系統
(3) 人員
(4) 基礎設施服務
(5) 實體區域
(6) 實體設備

【資通安全風險架構】

- 由本公司管理部吳副總負責督導、統籌資通安全及保護相關政策制定、執行，下轄資訊課副理負責主導及規劃；並帶領四位資訊工程師執行相關業務。



- 由各業務相關單位配合執行，以及稽核部門定期稽查與檢視資通安全各項業務的執行情形，每年會計師也會進行資訊環境風險評估與必要之控制測試，以評估年度公司資訊作業內部控制之有效性，以確認本公司資通安全管理運作之有效性。
- 資訊課負責制定資通安全管理政策，每月召開相關會議定期檢討修正，111 年共召開會議 12 次，並於每次會後將相關檢討與執行情形報告呈管理部吳副總審閱。
- 111 年度資通安全政策及具體管理方案執行情形已於 111 年 12 月 27 日在 董事會中報告。

【資通安全政策】

- 已於 2020 年 8 月訂定資訊安全政策，為確保資訊資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資訊安全管理體系。
- 資訊安全政策目標 ：

  維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

  (1) 保護本公司業務活動資訊，避免未經授權的存取、修改，確保其正確完整。

  (2) 尊重智慧財產權，保護顧客及公司資訊。

  (3) 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。

  (4) 定期進行內部與外部稽核，確保相關作業皆能確實落實。

  (5) 符合相關法令或法規之要求，達成業務持續運作之目標。

【資通安全控制措施】

- 每年定期盤點資訊資產清單，依資安風險評鑑進行風險管理，落實各項管控措施。
- 定期執行資訊安全宣導作業，每年辦理與資訊安全教育訓練，新進人員皆須簽定資訊保密協定。
- 所有員工、委外廠商暨其協力廠商須簽定保密聲明書，以確保使用本公司資訊以提供資訊服務或執行相關資訊業務者，有責任及義務保護其所取得或使用本公司之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。

- 重要資訊系統或設備應建置適當之備援或監控機制並定期演練，維持其可用性。
- 個人電腦應安裝防毒軟體且定期確認病毒碼之更新，並禁止使用未經授權軟體。
- 同仁帳號、密碼與權限應善盡保管與使用責任並定期換置。
- 制定資訊安全事件的回應及通報標準程序，以適當對資訊安全事件做即時處理，避免傷害擴大。
- 全體人員應遵守法律規範與資訊安全政策要求，主管人員應督導資安遵行制度落實情況，強化同仁資安認知及法令觀念。
- 考量資訊安全之風險不確定性，111 年度委由專業機構進行資安保險評估。

【111 年度執行情形】

- 本年度無發生重大缺失，亦無違反資通安全、造成客戶資訊洩漏及罰款等重大資安事件發生。

- 本年度共辦理 12 梯次資訊安全教育訓練(包含新進人員)，經理人及員工共計 322 人次參與。
- 於 10 月完成公司資訊系統災害復原演練。
- 本年度完成各項作業之資安保險評估，將於 112 年度安排電子郵件社交工程演練。