【資通安全對象與範圍】

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。

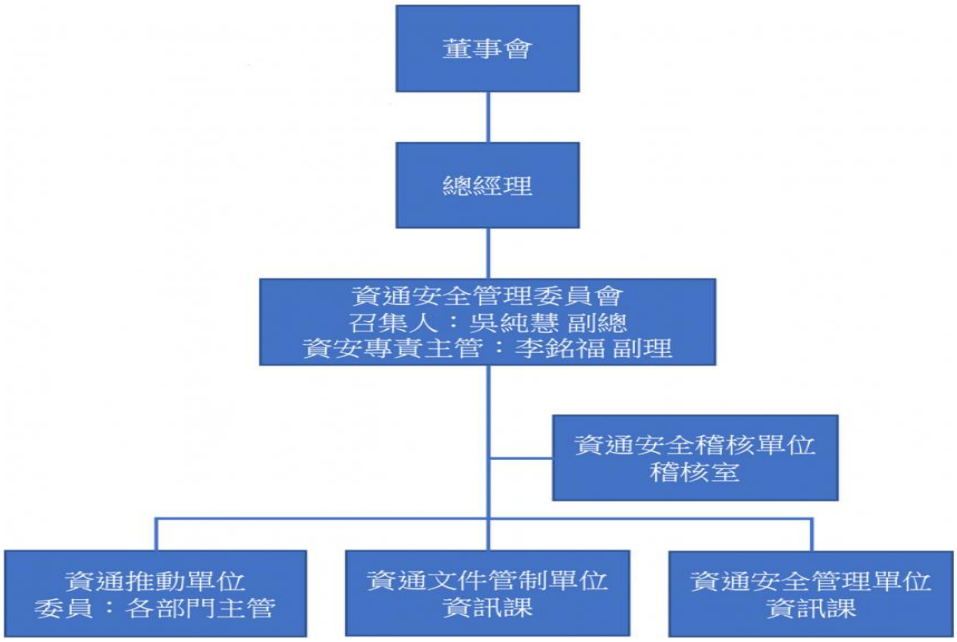
範圍：

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，己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:

- 資訊記錄
- 電腦系統
- 人員
- 基礎設施服務
- 實體區域
- 實體設備

【資通安全風險架構】

- 由本公司管理部吳純慧副總經理召集成立【資通安全管理委員會】，本委員會負責審視各業務單位之資通安全政策執行情形，以建構出資通安全防衛能力及同仁良好的資通安全意識，**112 年度資通安全政策及具體管理方案執行情形已於 112 年 12 月 29 日在董事會中報告。**



【資通安全政策】

為使五鼎各項業務順利運作，防止資訊或資通系統遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)，特制定本政策，以供全體同仁共同遵循：

(1)保護五鼎各項業務活動資訊之機密性與完整性，避免未經授權的存取、修改，確保其正確完整。
(2)因應資通安全威脅情勢變化，五鼎同仁應參與資通安全相關教育訓練，以提高企業資通安全意識。
(3)尊重智慧財產權，保護顧客及企業資訊。
(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。

【資通安全目標】

(1) 五鼎間接員工每年應完成 1 小時資通安全教育訓練。
(2) 若知悉資安事件發生，能於規定的時間完成通報、應變及復原作業(年度重大事件發生≤1 次)。
(3) 前次內部稽核發現事項，未完成改善之件數應≤2 件。
(4) 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。

【資訊安全控制措施】

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，落實以下各項管控措施。

- 定期執行資通安全宣導作業，每年辦理與資通安全教育訓練，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。
- 制定資通安全事件的回應及通報標準程序，以適當對資通安全事件做即時處理，避免傷害擴大。
- 考量資通安全之風險不確定性，每年定期執行電子郵件社交工程演練作業。
- 全體人員應遵守法律規範與資通安全政策要求，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。

【112 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。
- 本年度加入科學園區資安情資中心(SP-ISAC)及台灣 CERT/CSIRT 聯盟 (TW-ISAC)以即時收到最新資安情資並適時因應處置。
- 目前資通安全委員會成員共計 17 位，公司內各部門（包含稽核、管理、研發、工程、品保、財務）主管均為委員會成員。
- 本年度辦理資通安全委員會例行會議，共計 2 次。
- 本年度共辦理 11 梯次資訊安全教育訓練(包含新進人員)，經理人及員工共計 291 人次參與。
- 本年度委託外部資安廠商辦理 2 梯次電子郵件社交工程演練，第 1 次共 311 人次參與，郵件開啟率為 29%及附件點閱率 25% 超過資通安全訂定之目標;經加強教育訓練後第 2 次演練共 306 人次參與，郵件開啟率為 5%及附件點閱率 1%，已顯著下降，將每年度安排執行演練。
- 本年度委託外部資安廠商辦理五鼎資訊系統弱點掃描作業，已依結果進行弱點管控及規劃升級。
- 本年度於 7 月完成公司資訊系統災害復原演練。