【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。

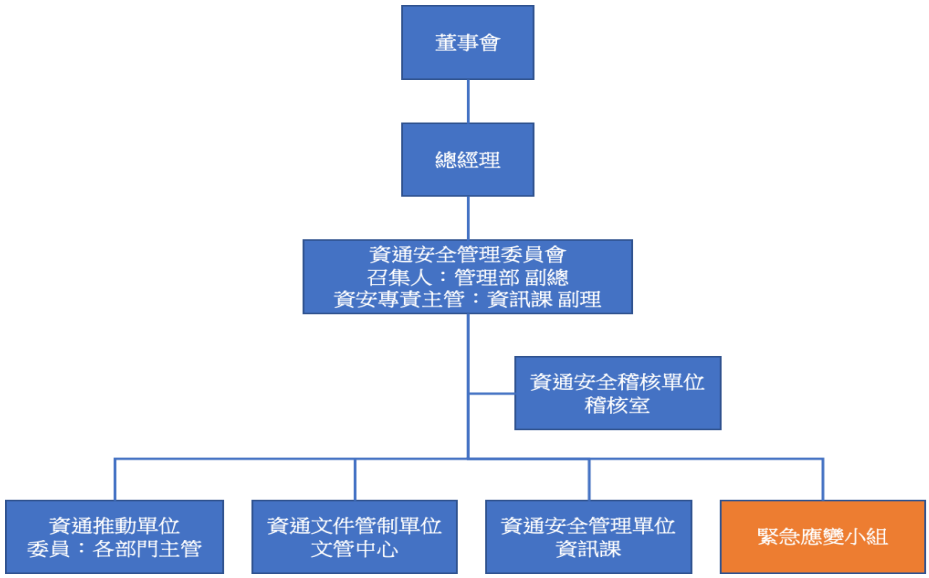
範圍：

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，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:

- 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 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，每年定期向董事會報告當年度執行情形。



【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) 強化人員資安意識，企業同仁應參與資安相關教育訓練，以提高全公司資安意識。

(2) 恪遵資安措施，各項資安管理作業與辦法，應切實遵守，並定期依實際狀況評估及調整。

(3) 避免機敏資料外洩，保護企業機敏資訊及資通系之機密性及完整性，避免未經授權的存取與竄改。

(4) 落實內部資安稽核，定期執行內部資安各項稽核措施，確保各項作業落實執行。

【資通安全目標】

(1) 資通系統操作人員每年應完成 1 小時資通安全教育訓練。

(2) 資安負責人員每年應完成 6 小時資通安全專業教育訓練。

(3) 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 ≤ 2 次; 通報、應變及復原作業比率為 100%)。

(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%。

(5) 於前次內部稽核發現事項，未完成改善之件數 ≤ 2 件。

【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。
- 內部稽核單位將資通安全檢查之查核列入每年稽核計畫必查項目。

【114 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。
- 已加入並持續關注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 4 次。
- 本年度委託外部訓練機構辦理 2 梯次資安負責人員教育訓練，共 3 人次參與。
- 本年度共辦理 11 梯次資通安全教育訓練(包含新進人員)，經理人及員工共計 303 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 303 人次參與，郵件開啟率為 7 %及附件點閱率 3 % 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 296 人次參與，郵件開啟率下降至 3.7%，已低於設定之郵件開啟率，附件點閱率則下降至 2.7%，將持續安排執行演練。
- 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。
- 於 9 月完成公司資訊系統災害復原演練。
- 本公司依據公開發行公司建立內部控制制度處理準則第 8 條、第 9 條規範訂定個人資料保護之管理及電腦化資訊系統等相關控制作業辦法，稽核單位亦將「資通安全」稽核項目排定於每年度稽核計畫內。114 年度內部稽核單位於 11 月中完成「 資通安全」稽核項目之查核，稽核結果為無缺失。