資通安全管理

(一)、資通安全風險管理架構:

- 本公司資通安全之權責單位為資訊部，負責統籌規劃、執行及推動資通安全管理政策，宣導並推展資訊安全意識，及蒐集和改進資通安全管理各層面上的管理、技術、程序與使用產品等。
- 本公司自111年度起設立專責專職之資訊安全主管及資訊安全人員各一名。
- 由稽核單位每年以內稽內控制度，進行資通安全查核，評估公司資通作業下的內部控制之有效性，並追蹤改善成效，以達到降低內部資安風險。

(二)、資通安全政策:

- 確保資訊安全三要素:機密性、完整性、可用性。
- 符合並依據各部門職能規範的資訊存取範圍。
- 維持確保各資訊服務系統的永續運作。
- 防範人為疏失、不當意圖及不法使用。
- 防止商業機密與機敏資料外洩的風險。
- 防止未經授權修改或使用資料與系統等。
- 維護資訊實體設備與相關周邊的環境安全。
- 定期執行資安稽核作業，確保資訊安全落實執行。

(三)、具體管理方案:

- 為因應突發狀況及資訊資料回復，已著手規劃資訊斷線備援演練及備援資產盤點。並透過演練來進一步了解目前欠缺的措施、設備、人員熟練等等應變能力，透過後續的補強規劃，來強化企業整體的應變能力與危機處理。
- 機房內主要伺服器設備與電力管理等，均定期配合廠商定期維護，保障防災、消防規劃、不斷電系統等保障維運環境。
- 使用次世代防火牆，將各內部需使用網路與服務的單位群組，進行分類與應用服務管制，加上時段管理與透過申請機制，來強化網路管理與彈性應用。
- 郵件服務搭配SPAM系統，並掛載防毒模組與進階防禦模組，系統程式會自動解封裝檔案進行掃描，可發掘潛在代碼、隱藏的邏輯路徑及反組譯程式碼，以利進行進階惡意程式比對。可進階防禦魚叉式攻擊、匯款詐騙、

APT 攻擊郵件、勒索病毒以及新型態攻擊等郵件。

- 資料檔案與系統面等備份，均安排排程自動化的定期備份，同時保留多個版本與異地存放。
- 使用伺服器虛擬化技術，透過系統備份機制，可在突發狀況發生時，將系統的歷程備份版本，進行快速系統掛載與服務恢復。
- 公司內所有的 Windows 電腦均有防毒軟體的佈建，並定期配合作業系統更新，能有效避免系統漏洞與提升系統安全，保障企業在整體應用上、網路上、管理上的可靠性與安全性。
- 公司內各系統的使用，同仁員工密碼原則上均不能少於8碼，並搭配特殊符號、數字、大小寫英文等，同時不能與歷程密碼相同。
- 定期宣導資訊安全政策與提供改善措施等規劃，避免內部同仁透過上網行為、郵件內容、USB 的隨插即用與個人持有設備等使用操作，造成公司內部風險提升與間接異常破壞。

(四)、投入資通安全管理之資源:

- 規劃與推動資安資訊人員每人每年安排資安專業課程訓練。
- 公司內所建置的防毒軟體、網路防火牆、郵件過濾等服務設備，持續使用並適時地進行軟、硬體之必要更新和升級。
- 111年系統開發及購置計畫:
  1. 新豐廠骨幹網路-核心交換器汰換專案。
  2. 郵件服務-SSL/TLS 的憑證購置專案。
  3. 備份管理-儲存設備規劃。
  4. 多因子認證導入專案。
  5. 提升端點防禦機制-EDR 模組規劃。
  6. 提報進行-資訊安全風險檢測。

(五)、列明最近年度集截至年報刊印日止，因重大資通安全事件所遭受之損失、可以影響及因應措施(如無法合理估計者，應說明其無法合理估計之事實):111年度無此情形。