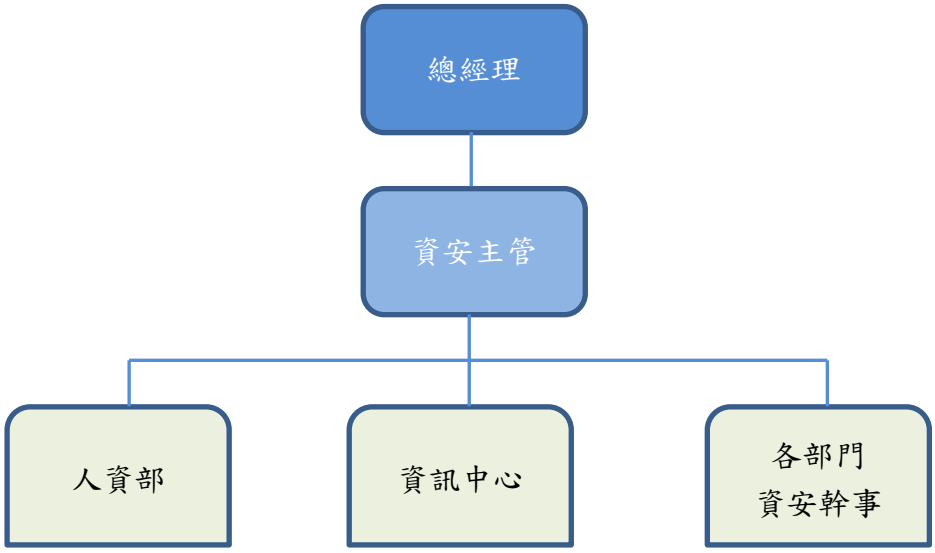
福華電子股份有限公司

2024 年資通安全管理執行情形

(一)資通安全風險管理架構、資通安全政策、管理方案及投入之資源

1. 資通安全管理組織架構



部門/職稱	職責
總經理	1. 明訂資訊安全管理系統範圍、組織架構、資源提供、持續改善等決策。 2. 指派資安專責主管。
資安主管	1. 負責推動本公司資安管理運作。 2. 確保資訊安全管理系統各流程的建立與維持 3. 監督資訊安全管理系統執行成效，包括改善的需求。 4. 監督內部稽核活動。 5. 設置資安主管 1 名。
資訊中心	1. 統籌資訊安全管理系統相關工作。 2. 統籌資訊安全管理系統相關人員培訓活動。 3. 負責資訊軟體體採購及管理，包括智財權管理。 4. 負責公司網路及資訊系統之建置及維運。 5. 負責資訊機房管理及維運。 6. 辦理資訊安全內部稽核活動。 7. 資安事件處理、發起及追蹤矯正措施活動。 8. 設置資安人員 1 名。
人資部	1. 人事管理。 2. 教育訓練。
各部門	1. 依公司資訊安全規定，執行各項活動、使用資訊設備及維護資訊安全環境。 2. 部門所屬資訊軟硬體設備、資訊系統、實體環境、人員、檔案資料等資訊安全管理與維護。 3. 相關供應商資訊安全之監督與管理。

本公司於 2019.9.12 即制定「福華電子公司資訊安全管理辦法」；辦法中明訂本公司資安風險管理組織架構及職責、資通安全政策、軟硬體存取控制程序、資訊作業管理、網路通訊管理、人力資源安全等相關作業標準進行遵循與管制。
在 2023 年設置資安專責主管和資安人員，負責統籌資安防護和相關政策執行及查核，確保公司個人資料保護、運營資料、資訊軟硬體設備和網路安全。

2. 資通安全政策、具體管理方案及投入資源

資安政策

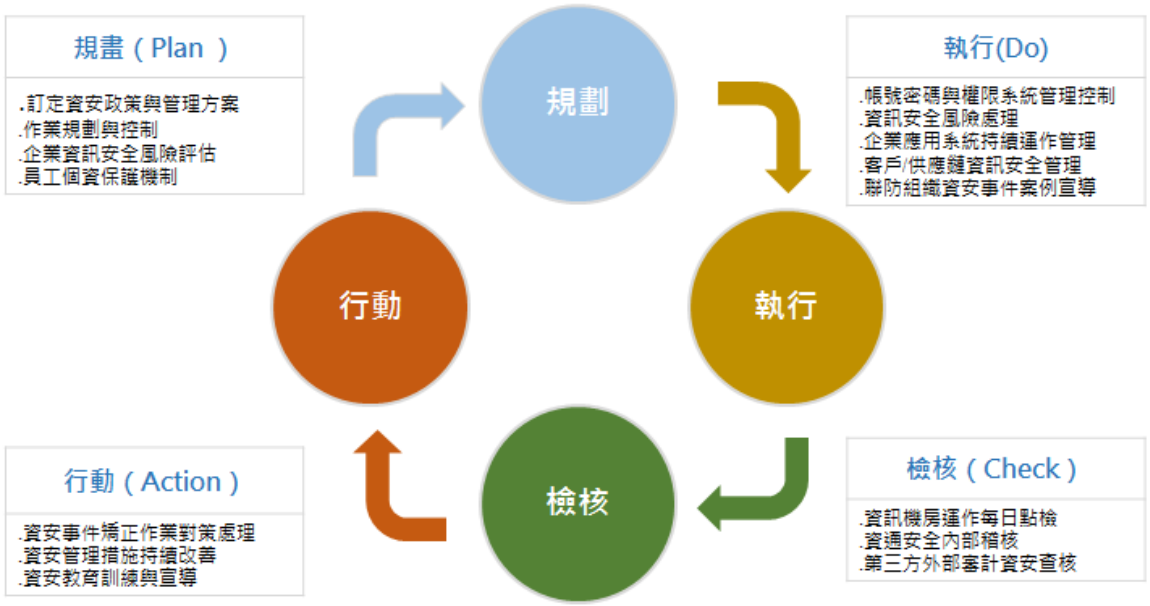
運用資訊科技保護公司的資訊資產安全
提供機密性、完整性及可用性資訊服務
創造公司、客戶及社會共好的資訊環境

在組織控制方面：

- 資通安全政策做為資安風險管理最高指導原則，同時依國內資通安全管控指引建立管理機制，確保資訊業務運作之有效性和持續性。
- 除建置資安防護外，並透過外部聯防組織或機構(如：台灣 CERT/CSIRT 聯盟、趨勢科技)提供威脅情報，分享相關資安情資，並做適當防禦以降低公司可能暴露之風險。
- 每季進行資安幹事會議，每年舉辦一次資通安全教育訓練。
- 稽核活動包含不定期之外部會計師事務所數位審計部門之資訊環境與資通安全查核，每年一次稽核室的資通安全內控檢查，以確定管理系統的實施狀況和是否達成各項資訊安全目標；查核報告併呈報董事長。
- 資安人員設置：資安主管和資安人員共 2 人；本年度防火牆、防毒軟體、SSL 憑證、ERP/NAS 備份裝置等投入費用約$900,000 元。
- 本年度資通安全管理報告並於 2024/11/21 董事會議呈報。

在技術控制方面：

- 依據 PDCA 循環的管理機制，落實資通安全政策施行：



- 落實資訊機房每日點檢，針對主要伺服器、防火牆 CPU 負載、郵件收發、專線流量、虛擬主機系統運作及負載等檢查。
- 建置防毒中控系統，提供主動性安全保護；並搭配第三方資安監控機制，防止電腦病毒入侵風險。
- 升級網路防火牆來達成網路防護與區隔，滿足內部需求並採取最小開放 port 原則，以強化關鍵基礎服務之安全管控。
- 擬定備份計劃並不定期進行備援可用性測試，例如企業 ERP 系統還原演練，確保系統完整性及高可用性，提供企業永續運作服務。

(二)重大資安事件影響及因應措施說明

最近年度及截至年報刊印日止，本公司並未發生造成公司或客戶損失之資訊安全事件。

對於資訊安全事件的通報與處理，本公司已明確訂立資安通報及處理流程並於員工資安教育訓練中揭示該通報程序；資訊中心接獲通報後需於目標處理時間內排除及解決資訊安全事件，並在事件處理完畢後進行原因分析與採取矯正措施，以預防事件重複發生。