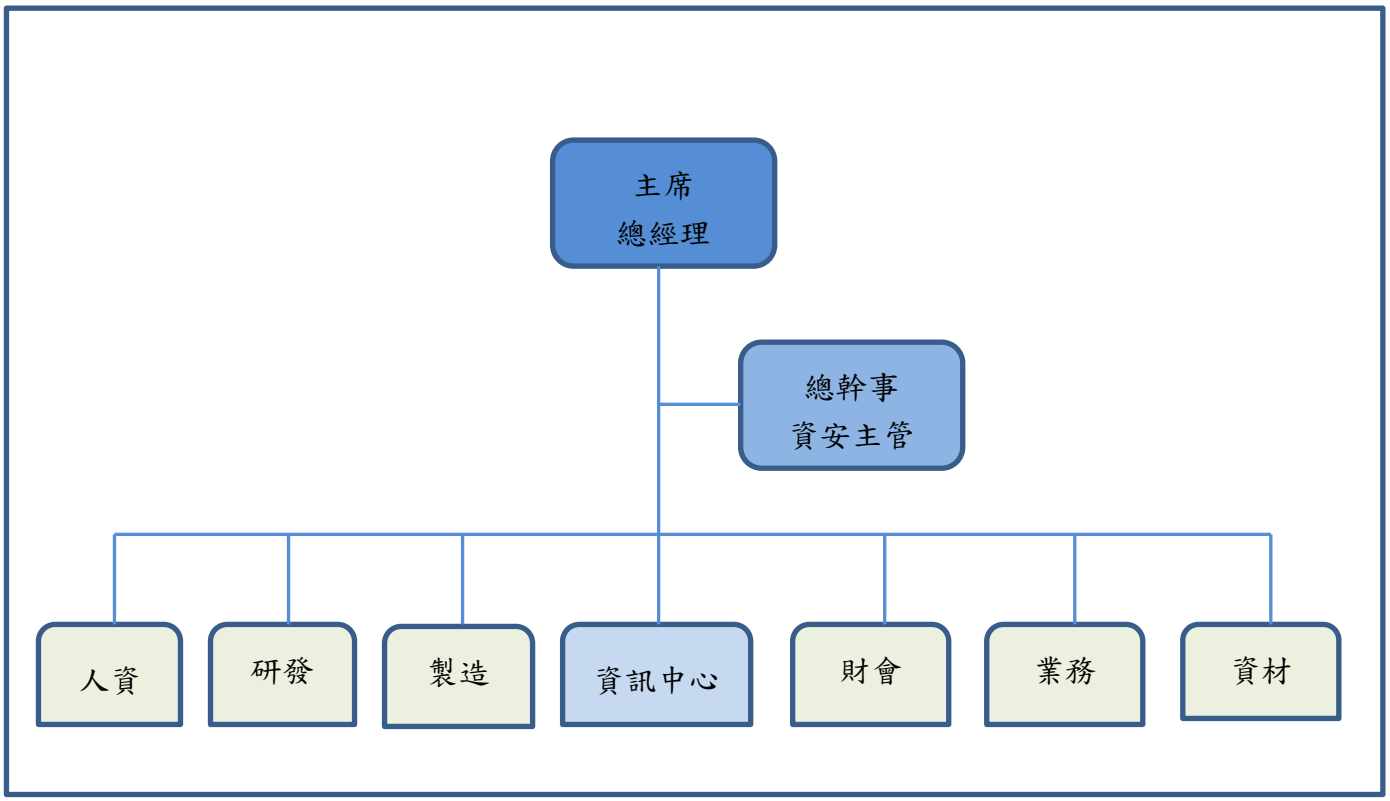
福華電子股份有限公司
2025 年資通安全管理執行情形

(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

本公司資安專責單位、資安主管已於2023年完成設置；於2025年組織本公司「資訊安全委員會」，由總經理擔任主席負責督導資訊安全及網路安全相關策略，並由資安主管統籌資安防護和相關政策執行，公司內各單位（包含資訊中心、人資、研發、製造、財會、業務、資材等）主管均為委員會成員。組織功能含蓋公司個人資料保護、公司運營資料、資訊軟硬體設備和網路安全，確保資訊安全管理體系持續運作的適切性及有效性。



依據「福華電子公司資訊安全管理辦法」，明訂本公司資安風險管理組織職責、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。

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。

部門/職稱	職責
	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。

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

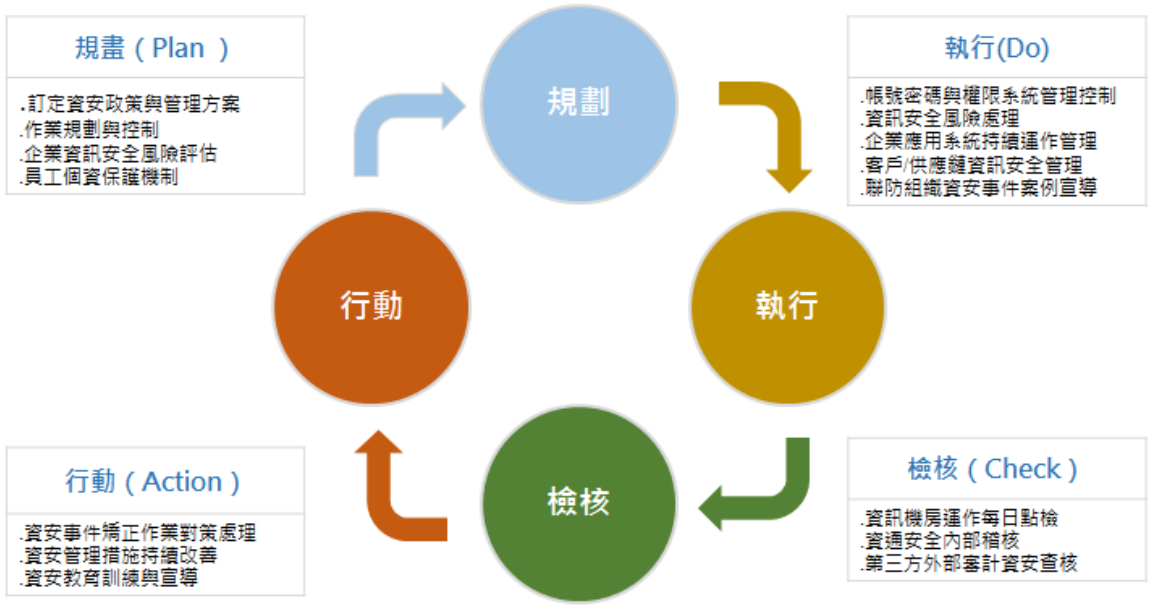
在組織控制方面：

- 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。
- 資安人員設置：資安主管和資安人員共 2 人。
- 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。
- 員工簽署個資聲明書，並告知當事人搜集個人資料之目的、類別以及當事人可行使之權利，以符合個資保護相關法令規定；每年並舉辦一次個資法常識宣導教育訓練。
- 外部協力廠商提供服務前，應簽署廠商保密同意書及承攬人個資告知同意書，並遵守相關資訊安全要求。
- 針對銷售客戶特殊重要交易事項，應簽署保密協議(NDA)，約束當事方同意不可揭露該項商業活動過程的任何敏感資訊，為交易資訊提供重要保護。
- 本年度 Microsoft 365 建置、固網防護、防火牆更新、官網上雲託管、防毒軟體、SSL 憑證、ERP/NAS 備份裝置等投入費用約$1,800,000 元。

- 本年度資通安全管理報告並於 2025/12/18 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。
- 固網續約採用 NGFW「次世代防火牆」技術，協助公司端於網路最前線阻擋惡意連線，直接阻斷駭客入侵攻擊與防護病毒威脅，保障企業資訊安全。
- 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。
- 更新網路防火牆達成區隔與提升網路防護能力，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。
- 公司官網上雲託管，由雲端供應商提供災難復原及防禦機制，除提升網站運行效率並減少內部網路遭受攻擊風險。
- 資訊系統操作採最小授權原則管制作業權限，避免未經授權之人員存取資料，防止個人資料/營業資料被竊取、竄改、毀損或洩漏。
- 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。
- 更新郵件系統，導入 Microsoft 365 雲端郵件平台，除提供使用者郵件存取便利性，並提升郵件服務系統之安全性與穩定性，有利整體資安環境。
- 預計導入 EDR「端點偵測與回應」技術，主動偵測終端設備上的異常活動，防止惡意軟體、未經授權的訪問，進一步提升企業網路系統安全。

(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。