

資通安全政策

一、政策目的

- (1) 幸康電子股份有限公司（以下稱「本公司」）為保障資訊資產及個人資料之安全，降低因人為疏失、蓄意行為、資訊系統異常、網路攻擊或天然災害等因素所造成之營運風險及可能損失，致力於建立並持續完善資通安全管理機制。
- (2) 本公司以維護資訊資產之機密性、完整性及可用性為核心原則，防止資訊及個人資料遭未經授權之存取、使用、洩露、竄改、毀損或遺失，並透過風險管理、安全控制、教育訓練、事件通報及持續改善等措施，提升整體資通安全管理效能。

二、適用範圍

- (1) 本政策適用於本公司全體員工、約聘人員、委外廠商及其他因業務需要使用、存取或管理本公司資訊資產之相關人員。
- (2) 本政策適用之資訊資產包括資訊系統、網路及相關設備、軟體、電子資料、文件、個人資料、帳號、存取權限及其他具有資訊價值之資源，並涵蓋相關資訊處理及業務活動。

三、資通安全管理目標

本公司致力於維護資訊資產之安全，確保資訊之機密性、完整性及可用性，並遵循相關法令及契約要求，持續提升資通安全管理與防護能力。政策目標如下：

- (1) 確保資通安全：防止資訊及個人資料遭未經授權之存取、使用、竄改或揭露。
- (2) 維持資通服務：採取適當之安全管理、備份及復原措施，維持資訊系統與業務運作之穩定。
- (3) 遵循法令要求：遵守適用之資通安全、個人資料保護相關法令及契約要求。
- (4) 提升安全意識：透過教育訓練及宣導，提升員工及相關人員之資通安全意識與防護能力。
- (5) 持續改善：持續檢視及改善資通安全管理措施，提升整體防護能力。

四、資通安全管理措施

為達成資通安全管理目標，本公司依資訊資產之重要性、營運需求及風險程度，建立並持續改善適當之資通安全管理措施，以維護資訊之機密性、完整性及可用性，確保資訊系統與業務運作之安全及穩定。

五、資通安全管理與執行機制

本公司設置資通安全管理小組，負責規劃及推動資通安全相關工作，並每年定期或視需要召開會議，檢視資通安全管理措施之執行情形及成效，推動安全檢查，建立資通安全事件通報與處理機制，並依實際需求適時調整相關資源，以落實資通安全管理。

六、資通安全事件通報與應變

- (1) 員工及相關人員發現疑似資通安全事件時，應儘速依公司規定通報。
- (2) 本公司應依事件性質及影響程度採取適當之應變、復原及改善措施，並依適用法令及相關要求辦理通報與處理。

七、資通安全教育訓練與人員責任

本公司全體員工及相關人員應接受資通安全教育訓練，遵守相關安全規定，並依其職責共同維護資通安全，確保資訊資產獲得妥善保護。

八、持續改善

本公司持續關注資通安全威脅、科技發展及相關法令之變化，定期檢視資通安全政策、管理制度及安全控制措施，並依風險評估及實際營運需求進行必要之調整與改善，以提升資通安全管理之有效性及組織營運韌性。