

盈正豫順電子股份有限公司  
資訊安全風險管理報告

日期:2024/11/4

前言:

公司之永續經營發展，向來重視投資人股東、客戶、供應商、員工、往來金融機構、政府組織、社區芳鄰等利害關係人之權益，除了導引良善公司治理、盡職企業社會責任，並輔以相應的內部控制制度、營運管理機制，以茲日常運行，達成公司營運的效果效率、財務報告正確允當、法令的遵循等目標。

隨著時代的進步、資訊的發展網路的延伸，資安風險也日漸升高，甚而影響企業的運作或財務、業務的損失。公司之於資安風險，業建置資訊安全風險營運管理機制因應，如「內部控制-資訊循環」、「內部重大資訊處理程序」、「防範內線交易管理作業程序」、「個人資料保護之管理」、「電腦作業管理辦法」及資訊安全管理系統作業程序書。2023年引進ISO27001資訊安全管理系統並驗證通過，提供所有員工落實遵循，以保障所有利害關係人之權益、公司經營之成果。

資訊安全管理機制

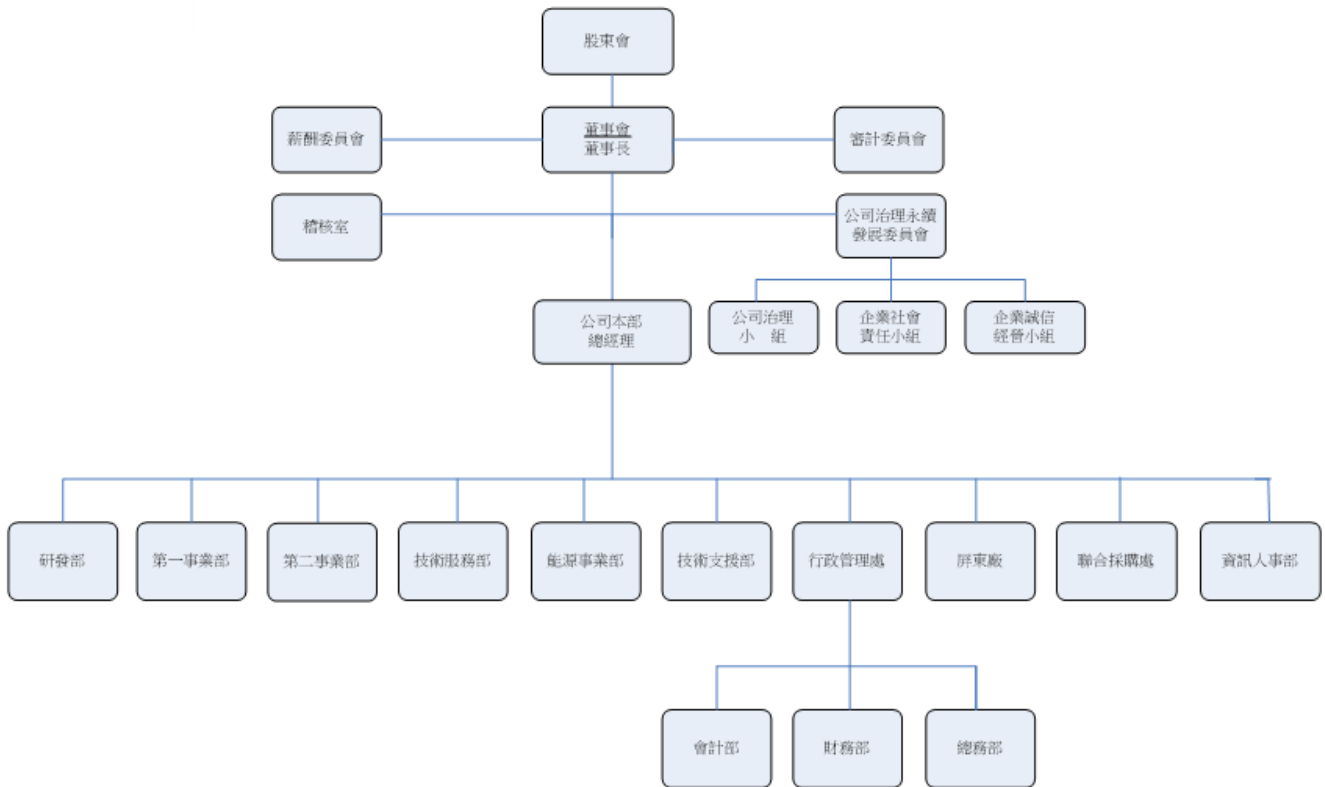
公司為永續經營發展之於資訊安全風險管理政策目標，以資安治理、法規遵循、科技應用等三大構面進行，強化本公司的資訊安全管理，建立「資訊發展，以安全為基礎」之觀念，確保客戶及同仁資料處理之機密性、完整性及可用性，務使本公司資料之處理全程均獲安全保障，提供安全穩定及高效率之資訊服務，並承諾落實運作與持續改善資訊安全管理系統。

資訊安全策略	
資安治理	實體及環境安全：確保組織的物理設施和環境受到適當的安全控制。 資產管理：管理組織的資產，包括識別、分類、追蹤和保護資產。 資訊安全事故管理：建立應對資訊安全事件和事故的策略和程序。 資訊備份：確保適當的資訊備份和恢復計劃。 資訊分類分級及處理：確保資訊按照其敏感性進行適當的分類、分級和處理。
法規遵循	網路安全：遵循相關法規和標準來保護組織的網路和數據傳輸。 保全開發政策：制定和實施適當的資安政策，以確保法規遵循。 技術脆弱性管理：監控並管理系統和應用程式的安全漏洞。
科技應用	資料傳送：確保數據在傳輸過程中受到適當的保護。 端點裝置之安全組態：管理和維護終端設備的安全配置。 密碼學：使用適當的加密技術來保護敏感資訊和通信。 技術脆弱性管理：綜合使用技術工具來識別、評估和處理脆弱性。

資安管理單位

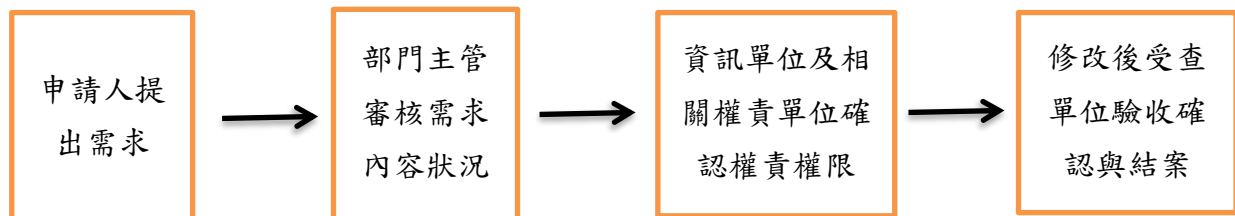
本公司資安管理單位為資訊人事部，負責審視公司各處分點資安治理政策、規劃、監督、資安管理運作情形，隨時監控各點資安情況。遇重大資安風險事件，及時向總經理報告，定期評估資訊安全風險並向董事會報告。

## 盈正豫順電子股份有限公司 組織圖



### 資訊服務流程管理

本公司各單位人員需求資訊應用軟硬體、系統、郵件、網路等資源權限之申請及異動，以電子流程申請程序，經有關權責主管審核、確認授權後辦理。



### 資訊安全管理方案

公司檢視資安風險經風險辨識與風險評估，確認該資安風險對企業經營不利之影響程度，採取相應管理措施，並針對資訊架構檢視、網路活動檢視、網路設備、伺服器及終端機等設備檢測、安全設定檢視等重點，隨時檢視及評估有無漏洞或設備老舊問題，也因應資訊安全所面臨的挑戰，如 APT 進階持續性攻擊、DDoS 攻擊、勒索軟體、社交工程攻擊、竊取資訊等資安議題，規劃資訊安全管理方案如下：

1. 風險評估：定期進行全面的風險評估，以識別潛在的威脅、弱點和風險。
2. 安全政策和程序：實施訪問控制、密碼策略、數據分類等要求。
3. 存取控制：實施身份驗證和授權機制，以確保只有授權的人員能夠訪問敏感資訊。
4. 網路安全：保護網路基礎設施，包括防火牆、入侵檢測系統、漏洞掃描和安全更新，以減少網路威脅。
5. 安全培訓和教育：為員工提供安全培訓和教育，以提高員工對資訊安全的認識。
6. 監控和警報：實施監控系統，以監視網路活動，及時檢測異常行為，以快速響應安全事件。
7. 事件應對計劃：制定安全事件的應對計劃和數據恢復策略，以減少損失並迅速恢復運營。
8. 定期審查和更新：定期審查和更新安全措施，以確保它們能夠應對新的威脅和漏洞。

## 資訊安全管理投入資源

項目	111 年度	112 年度	113 年度
防毒軟體	58,500	58,500	96,750
維護費用	2,210,687	2,363,149	2,209,711
機房門控費用	0	0	0
設備、軟體升級費用	2,675,750	3,259,830	4,653,578
總計	4,944,437	5,681,479	6,960,039

### 資安事件與保險

公司資安治理、管理機制之運行，於全體員工依據規定落實執行，並未發生嚴重資安事件，整體資訊安全風險管理得宜，可達預期目標。公司在實體資產已有保險、且主要檔案資料均採取異地備份，暨資訊系統災難恢復計畫，如未來法令規範、資安管理需求需投保資安險，屆時公司將評估了解其相關規定及配套措施再決定。

### 資安風險管理檢視與改善

公司管理階層依其職掌業務範疇以營運管理機制流程，進行資安內部控制實施與風險督導管理，及依年度實施風險內部控制制度自行檢查作業，進行資訊循環內部控制自行檢查作業，自行評估資安管理落實情形。且稽核單位並追蹤執行情形，每年度稽核計畫均納入查核項次，以確保落實及成效檢討或改善參考依據。

113 年度執行情形如下：

#### ◆ 導入機密文件存取控管系統

依據審計委員會暨董事會董事指示，為確保公司機密文件之安全性，避免公司資產存取到個人電腦不當使用或致外洩的風險，資訊安全管理需提升更為有效。本年度導入文件存取控管系統，提高了整體資料的安全性。

#### ◆ 定期進行系統更新

更新高雄 FileServer，台北 MailServer。修補系統已知漏洞。

#### ◆ 每年年底前定期複核使用者權限，以防止資料未授權的存取。

#### ◆ 使用集中式防毒系統 - 卡巴斯基，隨時監視病毒事件並排除。

#### ◆ 不定期宣導資安觀念。

近期，網路釣魚攻擊事件頻繁發生，並透過「噴灑與祈禱」(Spray & Pray) 方式針對企業員工進行攻擊。這類攻擊不僅利用電子郵件，還結合社交工程和假網站等多種手段竊取電子郵件帳號和密碼，進而導致郵件被濫用，甚至可能影響郵件系統的正常使用的。為應對這些威脅，企業必須加強員工的資訊安全意識培訓。藉此機會，我們再次強調不要點擊不明連結，有疑問時應立即向資訊安全相關人員求助，以避免成為攻擊目標。

報告人：資訊人事部經理 林岱明

(2024.11.4 提報公司審計委員會及董事會有關公司『資訊安全風險管理報告』核備。)