笙科電子股份有限公司

114 年度資訊安全管理執行情形

資通安全管理之資訊揭露

報告人：資安管理代表蔡合掌執行副總

董事會報告日期：114 年 12 月 24 日

Contents

1 資通安全管理策略與架構

敘明資通安全政策、資通安全風險管理架構、具體管理方案及投入資通安全管理之資源等。(法規依據：年報準則第18條第6款第1目)

1.1 資通安全政策

笙科電子股份有限公司的資訊安全政策涵蓋本公司及海內外子公司，是以「一、建立符合法規之資訊安全管理規範；二、透過全員認知，達成資訊安全人人有責的共識；三、保護公司資訊的機密性、完整性與可用性；四、提供安全的生產環境，確保公司業務之永續營運」為指導準則。並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

笙科電子股份有限公司已導入並建立完整的資訊安全管理系統（ISMS, Information Security Management System），從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求的資訊安全保護環境，並不斷地進行「計劃－實施－查核－行動」（PDCA, Plan-Do-Check-Act）循環以持續改善。

「計劃階段」著重資安風險管理，為了強化資訊安全，笙科電子股份有限公司自民國112年導入ISO27001資訊安全管理體系，使資訊系統皆能在標準的管理規範下運作，降低因人為疏失所造成的安全漏洞及生產異常，也透過年度的複審作業，不斷持續改善。

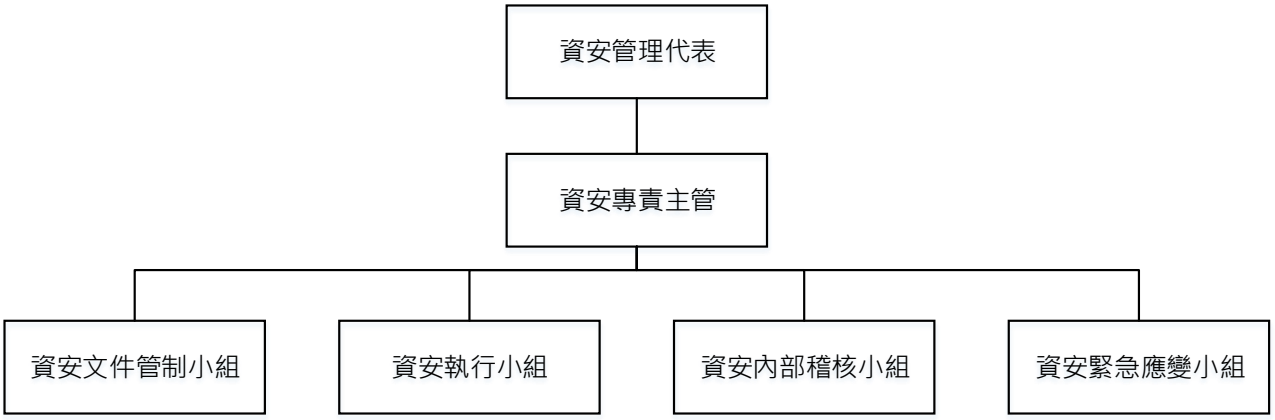
「執行階段」建構多層資安防護機制，持續導入新資安風險控管技術，以智慧化／自動化機制提升各類資安事件之偵測及回應處理程序的效率，並強化資訊安全及網路安全保護流程，以維護公司重要資產的防護。

「查核階段」定期監控資安管理指標成效，及上述管理系統每年第三方複審稽核，另委由知名的資安廠商進行滲透測試，以確保持續提升資安管理及防禦能力。

「行動階段」檢討與持續改善，透過年度的複審作業，不斷持續改善，提升資安管理及防禦能力。

1.2 資通安全風險管理架構

笙科電子股份有限公司在民國112年成立「資通安全管理委員會」負責執行資訊作業安全管理規劃，建置與維護資訊安全管理體系，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。



資通安全管理委員會組織圖

- 資安管理代表：由「執行副總」擔任。
- 資安專責主管：由「資訊服務部主管」擔任。
- 資安緊急應變小組：由「資訊服務部員工」擔任。

委員會每年向董事會報告資通安全管理審查會議之審查結果。

1.3 具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

- 法令遵循及導入國際資安認證標準：笙科電子股份有限公司推行資訊安全相關的ISO27001認證標準及法規，作為達成各項風險管理的方法與檢驗依據。公司內部亦成立對應的「資通安全管理委員會」，專責推動各項標準化作業，降低生產營運的風險。
- 提升資安防禦能力：定期進行資安系統脆弱度分析及滲透測試，並加以補強與修護，以降低資安風險。建立網路安全事件應變計畫，依事件嚴重度等級進行影響和損失評估，採取對應的通報及復原行動。
- 增進網路安全：整體資訊系統網路安全區域優化，增加重要主機特權帳號登入多因子認證防護。
- 教育訓練：進行全員資安教育訓練與不定期社交工程釣魚郵件測試，以提升資安意識，使資安的運作在高階主管與各部門的支持下，落實到每一位員工身上。

1.3.1 資通安全管理審查會議之審查結果

無重大議題

1.3.2 年度資訊作業查核

於 114 年 10 月，由勤業眾信聯合會計師事務所對本公司進行資訊作業查核。查核結果如下表。

編號	查核項目	發現與風險	建議	改善策略
(1)	系統變更控制	**發現事項：** 經查核發現 貴公司 1. Workflow ERP 主機(CORPAP03)及 AD 主機(CORPDC01)所在之 Windows 作業系統雖有進行作業系統 Patch 更新，但未填寫「資訊服務申請單」。 2. AD 主機(CORPDC01)所在之 Windows 作業系統未安裝微軟今年度釋出之重大更新，且未留有評估紀錄。 **風險：** 1. 若無落實 Patch 更新申請及測試驗收程序，則可能造成系統變更不當且無法被管理人員發現，進而影響系統資料正確性之風險。 2. 如未適時進行安全性更新，且未依系統狀況做出評估，恐導致漏洞無法即時修補，且易遭外部攻擊／威脅之風險。	建議 貴公司 1. Windows 作業系統進行 Patch 更新或升級時，應填寫「資訊服務申請單」，以留存申請及測試驗收紀錄並經主管覆核。 2. 應定期評估是否需安裝微軟發布之重大更新，若評估進行更新，應留存申請、測試及主管核准紀錄；若評估不需更新，則須留存相關評估紀錄。 註： 查詢官方 Patch 連結： https://portal.msrc.microsoft.com/en-us/security-guidance	1. 改為先填單後更新，以避免更新後未填單的狀況。 2. 每年三月及九月評估後填寫資訊服務申請單，並將評估結果列於申請單當中。
(2)	存取安全控制	**發現事項：** 經查核發現 貴公司 Check Point 防火牆 Authentication method: Check Point Password 之密碼原則未臻設置完善如下： 密碼期限設定：never expires 密碼最小長度:6 碼 **風險：** 若系統之密碼強度不足，且無定期變更密碼，則可能導致系統帳號較為容易被盜用，進而導致資料遭篡改之風險。	建議 貴公司 宜評估在不影響系統正常作業之狀況下，將 Check Point 防火牆之密碼原則，參照-S2-I-13 存取控制管理程序規範調整如下建議值： 密碼期限設定： 90~180 天 密碼最小長度:8 碼	密碼每 180 天更新一次並調整為 8 碼

1.4 投入資通安全管理之資源

- 建立符合法規之資訊安全管理規範
  - 導入 ISO27001 資訊安全管理體系
    - 相關會議開會次數: 6 次
  - 成立「資通安全管理委員會」
    - 資通安全管理委員會人員總數: 20 人
    - 資安執行小組上外訓課程

      IT Home 所舉辦之 CYBERSEC 2025 台灣資安大會

      台灣金融研訓院舉辦之資訊安全線上課程
- 保護公司資訊的完整性與可用性
  - 更新人事系統主機(存放所有虛擬機、M 資料、ERP 資料、電子簽核系統資料...)

    投入資金 NT$255,000
  - 更新備份主機及儲存空間

    (存放所有虛擬機、M 資料、ERP 資料、電子簽核系統資料...)

    投入資金 NT$390,000
- 防毒、防駭
  - 更新資安端點防護軟體

    投入資金 NT$360,000
  - 更新 Windows 作業系統 (Win7 -> Win11)

    更新 Windows 作業系統，投入資金 NT$93,000
  - 執行所有伺服器弱點掃描-滲透測試

    投入資金 NT$150,000
  - 執行社交工程演練，加強員工資安意識，避免執行惡意電子郵件。

    投入資金 NT$180,000

以上投入資通安全管理軟硬體之金額總和: NT$ 1,428,000

2 重大資通安全事件

本年度無重大資通安全事件發生。