笙科電子股份有限公司

113 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：113 年 12 月 25 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。

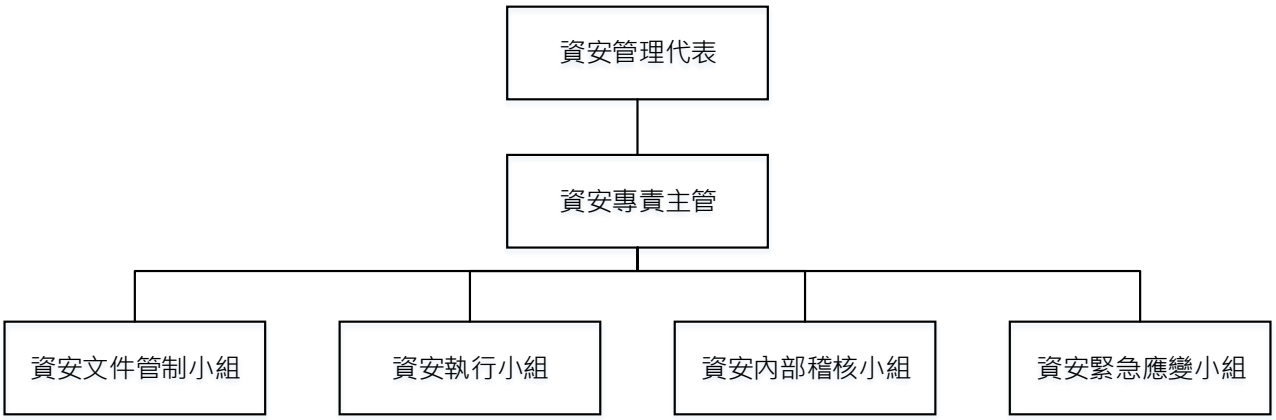
「執行階段」建構多層資安防護機制，持續導入新資安風險控管技術，以智慧化／自動化機制提升各類資安事件之偵測及回應處理程序的效率，並強化資訊安全及網路安全保護流程，以維護公司重要資產的防護。

「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

編號	稽 核 項 目	稽 核 發 現	改 善 策 略
4	其它	Window 7 作業系統過於老舊，微軟已不提供漏洞修補，有資安疑慮。	已於 2024 完成將有聯網能力電腦之 Windows 作業系統更新至 Windows 10、11

1.3.2 年度資訊作業查核

於 113 年 11 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。

<table>
<tr><th>編號</th><th>查核項目</th><th>發現與風險</th><th>建議</th><th>改善策略</th></tr>
<tr><td>(1)</td><td>系統變更控制</td><td>發現事項：
經查核發現 貴公司 Workflow ERP 主機(CORPAP03) 及 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，且未定期評估是否需要更新。

風險：
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。</td><td>建議 貴公司
應定期評估微軟發布之重大更新是否需更新，若評估不需安裝，則須留存評估紀錄及主管核准紀錄。</td><td>目前計畫採用 patch 更新系統(Ivanti)，每月做一次更新，系統預定 2024 年 12 月底會啟用上線。</td></tr>
<tr><td>(2)</td><td>存取安全控制</td><td>發現事項：
經查核發現 貴公司 Workflow ERP 系統連結之 MS SQL 資料庫以下帳號未套用 Windows 密碼有效天數設定，亦無人工定期變更密碼：
<table><tr><th>帳號</th><th>上次變更密碼日期</th></tr><tr><td>sa</td><td>2022/03/17</td></tr></table>
風險：
若密碼強度不足，恐導致系統帳號較為容易被盜用，進而提升資料遭竄改之風險。</td><td>建議 貴公司
為強化資訊安全，應評估於不影響系統運作之前提下，以人工方式定期變更密碼(至少一年一次)。</td><td>依建議每年以人工方式修改密碼。
(已於 12/5 更新密碼)</td></tr>
</table>

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: 5 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 2024 台灣資安大會

- 保護公司資訊的完整性與可用性
  - 建立軟體修補程式系統，用以管理、更新軟體修補程式

    投入資金 NT$320,000
  - 更新磁碟主機(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$700,000
- 提供安全的生產環境
  - 擴充機房 UPS(不斷電系統)並增加電源迴路

    投入資金 NT$69,720
  - 機房 UPS(不斷電系統)電池組更換

    投入資金 NT$65,000
  - 機房 UPS(不斷電系統)加固工程

    投入資金 NT$35,175
- 防毒、防駭
  - 防毒軟體授權

    投入資金 NT$630,000
  - 更新 Windows 作業系統
    - 更新 Windows 作業系統，投入資金 NT$448,000
  - 執行所有伺服器弱點掃描-滲透測試

    投入資金 NT$138,000
  - 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$138,600

2 重大資通安全事件

本年度無重大資通安全事件發生。