

笙科電子股份有限公司
112 年度資通安全管理執行情形

資通安全管理之資訊揭露

董事會報告日期：112 年 12 月 13 日

1	資通安全管理策略與架構	3
1.1	資通安全政策	3
1.2	資通安全風險管理架構	3
1.3	具體管理方案	4
1.3.1	資通安全管理審查會議之審查結果	4
1.3.2	年度資訊作業查核	5
1.4	投入資通安全管理之資源	6
2	重大資通安全事件	7

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。

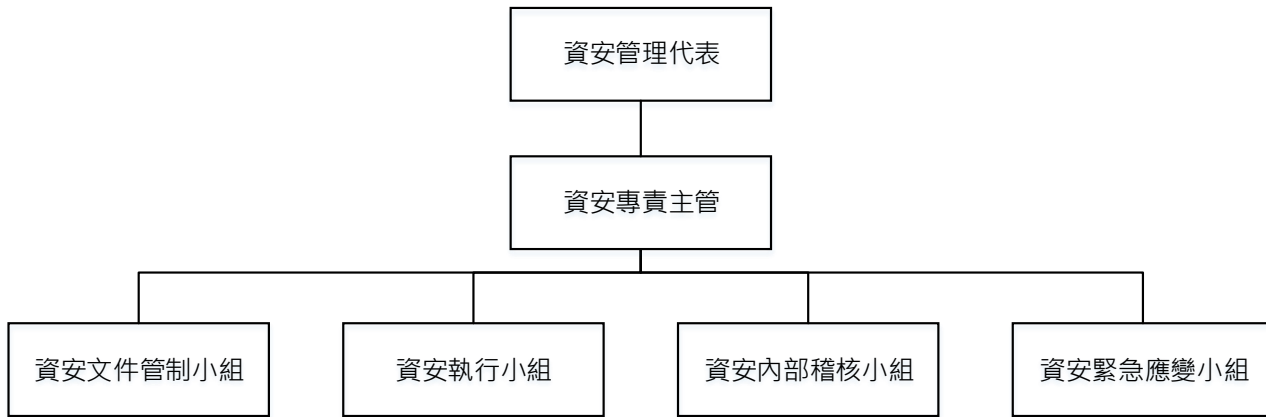
「**執行階段**」建構多層資安防護機制，持續**導入新資安風險控管技術**，以智慧化／自動化機制提升各類資安事件之偵測及回應處理程序的效率，並強化資訊安全及網路安全保護流程，以維護公司重要資產的防護。

「**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
1	S2-I-14 網路安全管理程序	查核防火牆未設定「網頁過濾」以防止內部連線至惡意網站。	啟用網頁過濾，並使用防火牆廠商所維護的惡意網站資料庫。

編號	稽核項目	稽核發現	改善策略
2	S2-I-13 存取控制管理程序	查核網域 Administrator 帳號未定期變更密碼。	將密碼期限設為 180 天。
3	S2-I-12 實體與環境安全管理程序	抽查備份系統主機未設定螢幕保護鎖定或登出系統。	全公司電腦設定為離開座位 15 分鐘
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。	更新 Windows 作業系統至 Windows 11

1.3.2 年度資訊作業查核

於 112 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。

編號	查核項目	發現與風險	建議	改善策略
(1)	系統變更控制	<p>發現事項： 經查核發現 貴公司 Workflow ERP 系統主機及 AD 網域主機所在之 Windows 作業系統更新未依照內控填寫填寫「資訊服務申請單」，以留存相關評估、申請及簽核紀錄。</p> <p>風險： 若無落實系統更新申請及測試程序，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。</p>	<p>建議 貴公司應落實作業系統更新申請程序，要求如有 patch 更新需求時，皆須透過相關單據提出系統更新需求，經資訊主管核准後執行。</p>	<p>落實作業系統更新申請程序，系統更新需求皆須經資訊主管核准後才可執行。</p>

編號	查核項目	發現與風險	建議	改善策略
(2)	存取安全控制	<p>發現事項： 經查核發現 貴公司 Check Point 防火牆密碼原則未臻設置完善如下：</p> <ul style="list-style-type: none"> 密碼期限設定：never expires <p>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。</p>	<p>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 防火牆密碼原則調整如下建議值：</p> <ul style="list-style-type: none"> 密碼期限設定：90~180 天 (或參照存取控制管理程序規範) 	<p>經與廠商討論後，升級防火牆管理系統，可達成密碼設定要求，故將升級防火牆管理系統，並將密碼期限設為 180 天。</p>

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
 - 聘請頂峰資訊顧問輔導，投入資金 NT\$600,000
 - 相關會議開會次數：17 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 2023 台灣資安大會
- 保護公司資訊的完整性與可用性
 - 建立 Mail server 備援
投入資金 NT\$235,000
- 防毒、防駭
 - 更新防毒軟體
投入資金 NT\$210,000
 - 更新 Windows 作業系統及老舊個人電腦
 - 更新 Windows 作業系統，投入資金 NT\$448,000
 - 更新老舊個人電腦，投入資金 NT\$629,160
 - 執行所有伺服器弱掃描-滲透測試
投入資金 NT\$138,000
 - 機房加裝監視器
投入資金 NT\$52,290

2 重大資通安全事件

本年度無重大資通安全事件發生。