精元電腦股份有限公司
113 年資通安全管理運作情形

(一)　資通安全管理策略與架構

1. 資通安全風險管理架構

(1)資通安全治理組織

本公司重視資通安全，由總經理督導本公司資訊安全管理制度、技術標準及維運作業之推行，指派資安主管統籌資訊安全工作推動。訂立資訊安全政策作為管理依據，保護員工、客戶、供應商及營運相關資訊資產之安全，確保企業永續經營。資安主管帶領資安維運組及資安應變組執行及管理總公司及子公司資安工作推動，定期舉行資安會議且向總經理提報資安相關議題，以落實與強化資安管理。最近期提報董事會資通安全執行情形日期為 113 年 12 月 24 日。

2. 資通安全政策

(1)企業資訊安全管理政策

依據 ISO 27001 國際資安管理標準，建立精元電腦資訊安全政策，各廠區遵循資安政策，考量當地的法規與業務規範，設定各廠資安目標，以滿足客戶對精元電腦資安的期望，致力於防範未經授權之存取、修改、使用及揭露等行為發生，確保企業之系統及網路維運達到機密性、完整性 與可用性等資安目標。每年檢視資訊安全政策與目標的適切性，並舉辦管理審查會議，進行資安議題探討與追蹤改善進度。

(2)企業資訊安全風險管理與持續改善架構

依據精元電腦資訊安全政策，以 PDCA 管理循環機制，落實資訊安全工作推動，防止違規及非法操作，持續給予員工資安教育訓練，主動進行風險弱點管理，確保實體環境安全、電腦主機安全、網路使用安全、系統存取安全、開發維護安全、移動與行動裝置安全， 對於員工違反資訊安全政策 時，按照公司獎懲辦法給予懲處並做為績效管理之參考依據，以降低資訊安全之風險，與對公司營運衝擊。

精元電腦極力推動 ISO 27001 國際資安認證，期望透過外部第三方公正單位 的稽核驗證，認證精元電腦對於資安的維運流程與規範，能達到國際的標準，滿足客戶對於精元電腦資安的期望。

(3)具體管理方案

強化公司員工資安意識：

1. 新進人員入職時簽署「員工使用網路規範」文件，包含資安防護事項，明確宣導員工應履行之義務及應遵守之資安規定並提醒同仁小心資安風險。

2. 定期舉辦資安教育訓練，對一般員工、管理幹部及資安專業人員進行資安授課，讓同仁明確清楚精元電腦資安管理相關規定，培養同仁資安意識且能遵守資安規定，教育訓練後進行一般考核，確保同仁學習成效，針對成效不彰的同仁進行加強教育訓練。

資安檢查：

1. 每年由總公司資安主管帶各廠各廠資安人員進行自評工作，參照上市櫃製造業資通系統安全指引及 ISO27001 等資安架構及控制項進行檢核，包含安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、物理與環境安全、操作安全、通信安全、資訊系統開發獲取與維護、供應商關係、資訊事件管理、持續營運管理及合規性的檢查。
2. 資安主管會將自評結果匯報總經理並送至稽核單位備存，並依風險程度要求各廠資安人員進行限時改善並經由複查通過後得以結案，落實 PDCA 管理循環機制。
3. 每年均接受客戶及外部第三方的資訊安全稽核，並依要求及建議修正及強化資安管理措施。

定期演練：

1. 對同仁進行社交工程釣魚郵件演練，針對演練結果針對高風險同仁進行資安安全教育訓練，提升資安意識。
2. 定期執行資訊系統資料備份及災難還原演練,並將演練結果匯報總經理。
3. 不定期進行系統異常運作、模擬網路攻擊、病毒感染等異常資安事件進行演練，確保同仁能即時處理與正確反應，保證營運不中斷。
4. 定期進行滲透測試，找出潛在的網路及系統弱點，進行修補與防禦。
5. 定期進行弱點掃描，檢查服務主機及終端電腦是存在漏洞，並落實弱點管理執行 Patch 更新動作，採取必要的漏洞修補或防護措施。

建構多層次安全防禦：

1. 網路安全: 網路准入管理、網路威脅監控(NDR)、內部威脅偵測防火牆
2. 端點管理: 防毒軟體、郵件防護、上網行為管控、端點威脅監控(EDR)
3. 最小權限: 訪問控制清單、堡壘機及特權管理帳號機制

(4)集團投入資通安全管理之資源

1. 資安人力: 集團現有 8 員專兼職資安人員(包含主管)。
2. 資安會議:113 年度集團招開資安相關會議計 194 場次(集團等級 14 場、廠區等級 180 場)，包含每年資安年會、每季 ISMS 管理審查會議，每月資安月會，每周資安例會，以落實資安管理。
3. 資安文件: 113 年度集團計有 9 份資安相關文件進行新增及修訂。
4. 社交工程演練: 113 年度集團執行乙次社交工程演練，發送 530 封信共有 33 員點擊。

5. 災難還原演練: 113 年度集團執行三次核心系統災難還原演練，完成資料備份檔及還原環境可行性驗證無誤。

資安目標:依據資安政策展開 113 年資安目標執行如下。
強化資安意識(已達成目標)：
- 全體同仁簽署員工行為準則達成率為 100%。
- 辦理社交工程演練，針對未通過同仁進行教育訓練， 完訓率為 100%。
- 提升同仁資安意識，資訊安全宣導次數共 6 次。

嚴守資安規定(已達成目標)：
- 蒐集資訊安全相關法規，並鑑定新增/修訂的法規，已完成執行。
- 檢視資通安全政策及目標的有效性，已完成執行。
- 每季舉行會議討論資安 ISMS 規範，檢討資安執行成效，已完成執行。

落實資安管理(已達成目標)：
- 公司重要主機進行弱點掃描每季一次，高風險嚴重弱點修補率為 100%。
- 終端電腦列入白名單並安裝防毒軟體得以使用網路，不符合件數 0 台。
- 病毒偵測數量達 10 個以上的電腦應開立處理單，未開單不符件數 0 次。

確保公司維運：
- 對外網路服務等級為 SLA99.9%。
- 為避免意外事件影響公司營運，進行業務持續演練(BCP)，已執行 5 次。
- 強化資安事件因應能力，規劃資安通報演練，已執行完成。

(二)重大資通安全事件
本公司於 113 年度未發生重大資通安全事件也未遭受損失。