台灣艾華電子工業股份有限公司

113 年資通安全風險管理執行情形報告

一、 管理架構：為提升資通安全管理，本公司由總經理為資通安全最高督導主管，指派資訊部為資通安全管理權責單位，並作為公司及子公司內跨部門資通安全治理、規劃、督導及推動執行，且每年定期向董事會報告當年度執行情形。

二、 資訊安全政策：

(1)恪遵法令訂定相關資通安全管理規章，對本公司資通資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。

(2)所有資訊安全事件或可疑之安全弱點，應及時依程序通報反映，並予以適當調查及處理。

(3)落實資訊安全教育訓練，確保員工認知資訊安全責任，以增進防護意識。

(4)落實遵守資訊安全相關法律及規定。

三、 資訊安全及管理方案

類型	說明	相關作業
權限管理	人員帳號、權限管理、系統操作管理措施	● 資訊權限申請單 ● 系統帳面修改單
存取控制	人員存取內外部系統、操作行為軌跡管理	● 操作行為軌跡軌跡管控措施(SmartIT、防火牆) ● 文件安全保護(D-Security) ● 內外部存取管控措施(SmartIT、防火牆、中華電信資安艦隊)
外部威脅	內部系統潛在弱點、病毒防護措施	● 病毒軟體防護與惡意程式偵測(ApexOne) ● 主機弱點偵測及更新措施(WSUS)
系統可用性	系統可用狀態、服務中斷處置措施	● 系統/網路可用狀態監控及通報機制(PRTG) ● 服務中斷之應變措施 ● 資料備份措施、本/異地備份機制(Veeam) ● 定期災害還原演練
資安通報應變	資安通報處理程序	● 加入TWCERT資安情資分享組織 ● 訂定資安事件應變處置與通報程序

四、 資通安全推行小組依據五大類資訊安全具體管理方案，投入資源如下：

(A)網路硬體設備：防火牆、中華電信資安艦隊服務。

(B)軟體設備：郵件防毒、垃圾郵件過濾、個人電腦端點防護、VPN 等。

(C)人力資源：每日系統狀態檢查、每日定期備份作業與異地副本備份、參加外部資訊安全課程與會議、不定期執行內部資安宣導。

(D)資安通報應變：加入 TWCERT 資安情資分享組織並訂定資安事件應變處置與通報程序。

五、 113 年度執行事項

(A) 資安事件

113/6 月中旬 SMTP 電子郵件攻擊

影響範圍：此事件屬服務負載攻擊無資料外洩情況，經查核為烏克蘭地區寄入大量垃圾郵件，導致公司電子郵件收發緩慢，設定 IP 黑名單阻止信件進入處置。

(B) 系統更新

每月 Windows 更新執行、D-Security 更新與升級 1 次、SmartIT 升級 1 次。

(C) 教育訓練

外部資安會議與課程 3 次、內部資安教育訓練 1 次。

六、 結論

1、113 年度本公司未發生重大網路攻擊事件，亦無客戶資料洩漏及違反資通安全等資安事件發生，也未曾涉入與資安相關的法律案件或監管調查。

2、113 年資通安全風險管理執行情形已於 113 年 11 月 6 日向董事會報告。