愛爾達科技股份有限公司

114 年度資訊安全風險管理運作情形

1. 資訊安全風險管理架構

本公司依據資訊安全政策成立資安小組，由總經理及各部門主管共四位成員組成，負責資安政策審核與相關制度規定之推動實施。並由資訊安全處共三位成員負責資安事務維運、訓練、宣導，事件損害評估與應變處理。每年至少一次由資訊安全處主管代表資安小組向董事會報告。(本年度於 11/4 董事會已報告)

2. 資訊安全政策遵循內部控制制度，制定管理規章辦法，推行教育訓練與落實管理程序，強化公司資訊基礎架構與設備安全以及系統與資料安全。

3. 資訊安全具體管理方案及實施狀況

具體方案	114 年度實施狀況
教育訓練與管理程序	1. 資安意識培訓計畫：定期於每年 6 月及 12 月舉辦資安意識培訓課程。 2. 資安測試：每年 2 次依上下半年不定期進行模擬釣魚攻擊，評估員工的識別能力，並提供釣魚郵件的相關培訓。 3. 資安政策宣導：透過內部郵件形式持續宣導資安政策。
基礎架構與設備安全	1. 定期漏洞掃描與修補：進行定期的漏洞掃描，並及時修補發現的漏洞，以確保系統的安全性。 2. 強化設備設定：確保所有設備使用安全的設定，包括適當的防火牆、密碼政策、登入限制等。 3. 定期更新與升級：確保所有系統和設備的軟體和硬體都得到及時更新和升級，以修補已知的安全漏洞。 4. 實施多層次防禦：建立多層次的安全防禦機制，包括防火牆、入侵檢測系統（IDS）、入侵防禦系統（IPS）等。 5. 實施存取控制：建立存取控制政策，限制對系統和資料的存取，只允許授權人員進行存取。
系統與資料安全	1. 加密敏感資料：對敏感資料進行加密，包括存儲和傳輸過程中的資料。 2. 建立災難恢復計劃：制定完整的災難恢復計劃，包括備份和恢復策略，以應對各種災難情況。 3. 實施資料監控：建立資料監控系統，定期監控資料的存取和使用情況，及時發現異常活動。 4. 定期資安審查：定期進行資安審查和測試，發現並修補系統和資料安全方面的弱點。
投入資訊安全管理之資源	依年度預算完成防火牆及防毒軟體續約，並視需求滾動式調整加購特定模組(如勒索病毒偵測防護模組)，皆遵循制度程序執行完畢。

4. 結論

檢視 114 年度各方案實施狀況，結果良好。並經外部稽核單位勤業眾信聯合會計師事務所與內部稽核單位查核各作業程序執行狀況，亦皆無重大異常。