

愛爾達科技股份有限公司

111 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。並由資訊安全處負責資安事務維運、訓練、宣導，事件損害評估與應變處理。

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 | 111 年度實施狀況 |
|-------------|---|
| 教育訓練與管理程序 | 每季執行資訊安全宣導與不定期之教育訓練。 維持軟體公司資安資訊分享，並確保緊急支援管道。 (三) 無發生資安緊急事件。 |
| 基礎架構與設備安全 | 使用防火牆阻擋來自外界的惡意攻擊，計每月阻止約有 1 百萬次的惡意嘗試登入次數。 每工作日執行機房檢查並記錄電腦機房進出工作表。 依實際進出狀況紀錄於機房進出人員登記表。 (四) 不定時依任務需要或專案需求，進行資訊設備採購案，皆循制度程序執行完畢，且重要設備均造冊管制。 |
| 系統與資料安全 | 使用防火牆阻擋來自外界的惡意攻擊，計每月阻止約有 1 百萬次的惡意嘗試登入次數。 每工作日執行機房檢查並記錄電腦機房進出工作表。 依實際進出狀況紀錄於機房進出人員登記表。 (四) 不定時依任務需要或專案需求，進行資訊設備採購案，皆循制度程序執行完畢，且重要設備均造冊管制。 |
| 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 111 年度各方案實施狀況，結果良好。並經外勤業眾信聯合會計師事務所與稽核部查核各作業程序執行狀況，亦皆無重大異常。