誠泰工業科技股份有限公司
112 年度
資訊安全風險管理運作情形

一、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、資安專責主管及各部室主管組成，負責資安政策審核與相關制度規定之推動實施。並由資訊部負責資安事務維運、訓練、宣導，事件損害評估與應變處理，每年定期向董事會報告資訊安全政策具體實施狀況。

二、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。

三、資訊安全具體管理方案

具體方案	實施內容
教育訓練與管理程序	1. 遵循法規規定與內控制度規章執行各項程序作業。 2. 每年需實施資訊安全教育訓練與宣導說明資安事件範例。 3. 每年資訊部同仁須參加資安相關訓練與研討會。 4. 須及時處理資安事件並進行事件分析與問題排除。 5. 須建立並維持緊急支援管道。
基礎架構與設備安全	1. 依循規定造冊管理相關資訊資產設備並定期盤查。 2. 每工作日執行機房檢查並記錄機房工作日誌。 3. 依實際進出狀況紀錄於機房進出人員登記表。 4. 確保各系統主機與網路設備運作無異常。 5. 持續偵測管控各項異常狀況並予以適當因應。
系統與資料安全	1. 每工作日執行資料備份並記錄於備份作業點檢表。 2. 每季執行備份復原演練。 3. 依辦法規定程序執行人員異動之權限增刪作業。 4. 每年 12 月份須進行年度權限盤點。 5. 按時進行作業系統功能與安全性更新。 6. 每年須執行年度個人電腦安全檢查。 7. 需按規定程序處理程式開發申請案。

四、實施狀況

具體方案	112 年度實施狀況
教育訓練與管理程序	1. 確循制度規章執行各項程序作業。 2. 執行 1 次資訊安全教育訓練，3 次資訊安全宣導。 3. 資訊部同仁參加 10 場資安相關訓練與研討會。 4. 本年度未發生資安緊急事件。 5. 維持科學園區資安資訊分享與分析中心(SP-ISAC)、台灣電腦網路危機處理暨協調中心(TECERT/CC)以及 5 間外部廠商關係，確保緊急支援管道。

誠泰工業科技股份有限公司

112 年度

資訊安全風險管理運作情形

基礎架構與設備安全	1. 依實際異動狀況即時更新資訊資產清冊，並於年終執行盤點作業。 2. 確實執行每工作日執行機房檢查並記錄機房工作日誌。 3. 確實執行依實際進出狀況紀錄於機房進出人員登記表。 4. 各系統主機與網路設備運作皆無異常。惟電簽系統有進行升版(24.0->25.5)以修補系統漏洞。 5. 因應資安風險採取主動預防策略，今年度列入 784 個疑慮 IP 來源至防火牆黑名單做預防管制。此預防性作法，有效降低異常 IP 持續性異常探測狀況。
系統與資料安全	1. 每工作日執行資料備份並記錄於備份作業點檢表，且於研發大樓存放異地備份資料。 2. 完成每季 1 次備份復原演練，全年度共執行 4 次演練保持應對能力。 3. 依辦法規定程序執行人員權限異動作業，截至報告日止共 23 次。 4. 於 12 月份執行年度權限盤點，並依新年度人事派令更新配置適當權限。 5. 依作業系統原廠進度實施功能性與安全性系統更新。 6. 於 6 月份執行年度個人電腦安全檢查完畢。 7. 按規定程序執行程式開發作業並設置合適權限，截至報告日止共 14 件次。

五、結論

檢視全年度各方案項目實施狀況，皆遵循法規與制度辦法要求執行，並視實際資安情勢適當應對，整體結果良好，無重大異常。