

威鋒電子股份有限公司

資訊安全管理政策

第一章 目的

威鋒電子股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保資料、系統、設備、網路安全及所屬之資訊資產的機密性、完整性、可用性與適法性；並符合相關法令、法規與合約之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本公司之業務需求，訂定本政策。

第二章 範圍

本政策適用對象包括本公司所有同仁及有權限進入本公司之集團人員、保全、臨時人員、替代役、委外服務廠商及訪客。

資訊安全管理之範疇涵括 14 個領域，避免因人為疏失、蓄意或天然災害等因素，對本公司造成各種可能之風險及危害，各領域分述如下：

1. 資訊安全政策。
2. 資訊安全之組織。
3. 人力資源安全。
4. 資產管理。
5. 存取控制。
6. 密碼措施。
7. 實體及環境安全。
8. 運作安全。
9. 通訊安全。
10. 資訊系統獲取、開發及維護。
11. 供應者關係。
12. 資訊安全事故管理。
13. 營運持續管理之資訊安全層面。
14. 遵循性。

第三章 資安管理指標

為維護本公司資訊資產之機密性、完整性、可用性與適法性，並保障客戶資料之安全，期藉由本公司全體同仁共同努力以達成下列資訊安全管理目標：

1 資訊架構檢視

1.1 檢視本公司資訊資產相關措施之架構與維運機制是否存在單點失效之風險，及針對業務持續運作之妥適性進行風險分析，並提出資訊架構安全評估之結果與建議，若非在風險承受度內，則研議與執行改善之方案。

2 網路活動檢視

2.1 檢視本公司網路設備、資安設備及伺服器之存取紀錄、帳號權限之授予與監控機制是否符合內控作業規範；並清查相關設備之帳號權限及存取紀錄，識別異常紀錄與確認警示機制。

3 公司網站、網路設備、伺服器及終端機等設備安全檢測

3.1 定期或適時進行公司網站、網路設備、伺服器及終端機的弱點掃描，並針對所發現之弱點進行改善、修補作業。

3.2 評估弱點掃描作業之範圍、作業模式及弱點改善計畫與修補情形，針對掃描結果提出評估建議，重點在於找出公司整體資訊資產環境中可能存在的弱點與漏洞，予以改善及修補，降低整體之資安風險。

4 安全設定檢視。

4.1 包含伺服器端與使用者端的安全性控管。

4.2 定期檢視伺服器端(如：網域服務 Active Directory)與使用者端(如：「密碼設定原則」、「帳號登入失敗鎖定原則」、「螢幕保護鎖定原則」等)的安全性設定，並透過控管工具管理及查核作業，檢視公司相關網域安全性原則設定是否符合內控規範。

5 資訊安全教育訓練與社交工程演練

5.1 針對本公司全體同仁，於內部安全監控範圍內，寄發測試郵件，並宣導及強化資通安全教育。

5.2 主要評估項目為：

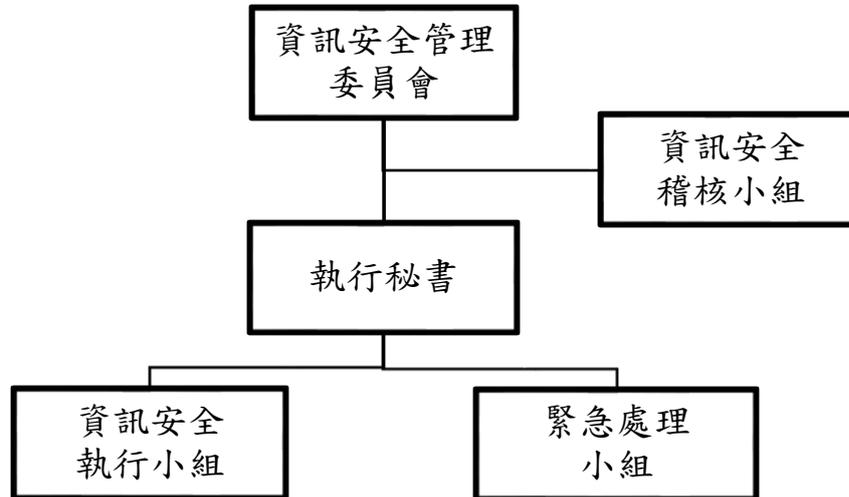
(一)定期舉辦資訊安全教育訓練講座及公告宣導。

(二)社交工程郵件演練測試郵件之開啟率及點閱率。

(三)後續改善機制演練目標，主要在於讓同仁瞭解使用電子郵件之風

險，提高同仁防範社交工程攻擊之危機意識。藉由持續演練以降低社交工程攻擊所造成之風險，進而達到保護本公司與客戶資料及重要營運資訊與服務之目的。

第四章 資訊安全組織架構與工作職掌



- 1 資訊安全管理委員會：
 - 1.1 本公司設「資訊安全管理委員會」（以下簡稱本會），負責資訊安全政策推動事宜。
 - 1.2 召集人：由本公司副總經理(本公司資訊安全長)擔任，並為會議主席，綜理本公司資訊安全政策之推動、協調及督導。
 - 1.3 委員：各部門主管為當然委員。
 - 1.4 本會每半年應至少召開一次資訊安全管理審查會議，審查資訊安全管理相關事宜。
- 2 執行秘書：
 - 2.1 由召集人指派一部門主管(本公司資訊安全官)擔任之。
 - 2.2 負責資訊安全作業之監督與審核工作。協調資訊安全執行小組執行資訊安全及緊急事故處理等相關作業。
- 3 資訊安全執行小組：
 - 3.1 組長1人，由資訊安全官指派人員。
 - 3.2 小組秘書，由小組組長指派人員。
 - 3.3 小組成員，由各部門主管指派資訊能力較佳之正職人員擔任。
 - 3.4 負責擬訂資訊安全管理相關規範，推動與執行資訊安全相關工作，執行資安推動委員會決議事項。
- 4 緊急處理小組：為任務編組，由資訊安全官指派人員組成。
 - 4.1 設組長1人，由資訊安全官指派人員。
 - 4.2 當重大資安事件發生時，負責聯絡及召集緊急處理小組。並且協調及督導各關鍵業務流程負責人執行作業和協調資源之調派使用。

- 5 資訊安全稽核小組：
 - 5.1 設組長1人，由稽核兼任。
 - 5.2 小組成員由各單位資訊聯絡人中選派組成。
 - 5.3 負責資訊安全管理制度執行情形之稽核。

第五章 資訊安全管理責任

- 1 本公司由「資安管理委員會」統籌資訊安全政策之推動與管理事項。
- 2 本公司各級主管應積極參與資訊安全相關活動，並支持資訊安全業務。
- 3 本公司各級主管對本政策及相關資訊安全管理規範負督導執行之責。
- 4 本公司所有同仁，有權限進入本公司之集團人員、保全、臨時人員、替代役、委外服務廠商及訪客應遵守本政策及相關規範，恪盡保護本公司資訊資產安全之責，並有責任透過適當通報機制，通報資訊安全事件或資訊安全弱點。
- 5 任何危及資訊安全之行為，將視情節或疏失輕重，依本公司之相關規定進行議處或追究其法律責任。

第六章 資訊安全政策之評估及實施

- 1 本政策應每年定期進行評估，以反映本公司資訊安全管理政策、相關法令規範、環境及公司業務之最新狀況，以確保資訊安全實務運作之可行性及有效性。
- 2 本政策奉董事會核定後實施，修訂時亦同。
- 3 本辦法制定於中華民國 108 年 11 月 15 日。