

聯上開發股份有限公司

資訊安全管理作業辦法

第一條、目的

為確保公司電腦之資料、設備、系統、網路的正常運作，資訊傳輸之安全，及電腦處理資料之機密性與完整性，特訂定本辦法。

第二條、權責及權限

- (一) 資訊系統安全控制由行政部資訊管理人員負責辦理。
- (二) 資料及資訊系統之安全使用及保護事宜由各部門負責辦理。

第三條、範圍

- (一) 電腦系統安全之管理
- (二) 網路安全之管理
- (三) 系統存取控制之管理
- (四) 系統發展及維護之管理
- (五) 資訊資產、實體及環境安全之管理
- (六) 業務永續運作之管理

第四條、電腦系統安全之管理

資訊管理人員應採行必要的事前預防及保護措施，偵測及防制電腦及其他惡意軟體，確保系統正常運作。並依相關法規或契約規定使用軟體。

第五條、網路安全之管理

- (一) 開放外界連線作業之資訊系統，應視資料系統之重要性，採用資料加密、身份鑑別、電子簽章、防火牆等措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
- (二) 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未同意之個人隱私資料及文件，不得上網公布。
- (三) 機密性資料及文件不得以電子郵件或其他電子方式傳送。
- (四) 不得隨意下載及安裝來路不明或私人軟體，暨不得利用公司網路資源閱覽或傳送有關色情、政治或與業務範圍不相關之文字或圖片，違反者依工作規則議處。
- (五) 公司所有之個人電腦未經資訊管理人員許可不得任意拆裝或私自攜帶外出。

第六條、系統存取控制之管理

- (一)離(休)職人員，應立即取消各項資訊資源之所有權限，並列入離(休)職之必要手續，人員職務調整及調動，應依系統存取授權規定，調整其權限。
- (二)對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並課其安全保密責任。

第七條、系統發展及維護之管理

- (一)資訊管理人員於自行開發或委外發展系統，應在系統生命週期之初始階段，將資訊安全需求納入考量，系統維護、更新、上線執行及版本異動，應予安全管制，避免不當軟體及電腦病毒等危害系統安全。
- (二)委託廠商建置及維護重要之軟硬體設施，應在公司資訊管理人員監督及陪同下始得為之。

第八條、資訊資產、實體及環境安全之管理

- (一)資訊管理人員建立與資訊系統有關之資訊資產目錄，訂定資訊資產項目、擁有者及安全等級分類等。
- (二)資訊管理人員應定期維護保養及測試各項電腦設備安全，並加以記錄。
- (三)電腦機房及各項電腦軟硬體設備應強化設(放)置處及防護措施避免遭致水患、風災、火災等災害並定期檢測消防安全設備。
- (四)電腦機房應實施門禁控管，進出機房人員應予記錄，維護人員應由電腦資訊管理人員陪同，始得進出管制區域。

第九條、業務永續運作之管理

- (一)電腦資訊管理人員應評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序。
- (二)如因資訊安全事件(包括系統有安全漏洞、遭受非法入侵或破壞、遭遇阻斷服務攻擊及功能不正常事件等)，致電腦系統無法運作或影響執行效率時，相關人員應視其嚴重程度及影響層面呈報權責主管。

第十條、訂定與施行

- (一)本辦法未盡事項，依主管機關及公司相關規定辦理。
- (二)本辦法之訂定與修正應經董事會決議，並於通過後實施。
- (三)本辦法訂定於民國一〇三年十二月二十四日。