易華電子股份有限公司

資訊安全政策

1.目的(Purpose)：

為維護整體資訊安全，強化各項資訊資產之安全管理，確保具機密性、可用性、完整性，已因應業務運作需求，特訂定本政策。

2.適用範圍(Scope)：

(1)適用於組織內資訊使用者與各項資訊資產。

(2)資訊使用者係包含正式員工、建置維護廠商及其他經授權使用資訊資產人員。

(3)各項資訊資產係包含安全管理政策、物理實務安全、人員管理安全、安全規章法律、硬體設備安全、軟體系統安全、網路通路安全。

3.作業說明(Operating Requirement)：為保護資訊資產安全，應建立資訊資產清冊並分類分級。資訊資產分為、硬體類資產(如電腦硬體、通訊設備等)、軟體類資產(如應用軟體、系統軟體等)。

(1)人員安全：為降低內部人為因素對資訊安全之影響，各單位應考量人力與工作職掌，實行分工。應視需要實施資訊安全教育訓練及宣導，以提高人員對資訊安全之認知。

(2)實體安全：

a.訂定電腦機房管理作業原則：

*機房內設備例行性檢查。

*機房內資訊設備及資訊媒體使用管理注意事項。

*門禁管理。

b.訂定辦公區域管理作業原則：

*桌面整潔管理。

*離開電腦作業設定螢幕保護程式。

*一般設備安全管理。

c.訂定一般資訊設備管理作業原則：

*個人電腦管理。

*個人電腦報廢。

d.主機系統安全：為確保主機作業平台及資料庫之安全，使操作程序標準化，應訂定主機操作與異常處理日誌。主機系統係指大型電腦、伺服器、資料庫等。

作業平台係指Windows Server、Unix及網站伺服器等。

e.應用系統安全：

為確保應用系統開發、測試、上線及維護之安全，應訂定標準管制及驗收程序、應用管理系統開發管理、應用系統驗收測試、應用系統上

線作業及應用系統維護。應用系統係指管理資訊系統及應用服務系統。

f. 網路安全：為確保網路服務及使用之安全，應訂立管理規範。

g. 訂定網路安全管理作業原則：

*網路設備安裝維護事宜。

*防火牆建置與管理作業原則。

*網路安全監控檢核原則。

*電腦病毒防治注意事項。

h. 存取安全：

為避免資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限。資訊存取控制作業原則包括：

*使用者存取權限區分與管理。

*主機平台使用者帳號密碼管理。

*網路設備系統管理員帳號管理機制。

*筆記型電腦連線管理機制。

*無線裝置、攜帶式行動設備等使用管理機制。

i. 資訊安全事件管理：

為降低資訊安全事件造成之損害，應建立資訊安全通報及處理程序，並加以記錄，包括：

*內部危安事件：發現(或疑似)遭惡意破壞毀損、作業不慎、資料遭竊等。

*外部攻擊事件：病毒感染事件、駭客攻擊(或非法入侵)事件。

*天然災害事件：颱風、水災、地震等。

*重大突發事件：火災、爆炸等。

*建立資訊安全事件通報程序。

*建立資訊安全事件分析及處理程序。

*資訊系統、資料之備份作業。

*災害復原計畫。

j. 業務永續運作管理：

為避免資訊資產遭受災害而影響業務永續運作，訂定應變及復原計畫，並不定期測試演練。訂定業務永續運作管理作業原則：

*災害處理程序。

*備份資料異地儲存程序。

*應用系統回復處理程序。

*關鍵業務之復原優先順序。

*分析業務停頓的損失和備援措施。

*在地備援管理規範。

4. 本政策經總經理核定後公告實施，修正時亦同。