

彰化第六信用合作社資訊安全政策

112年1月17日理事會通過訂定

- 一、本社為確保本社資訊系統、資料、設備及網路之安全，特訂定本政策。
- 二、資訊安全之定義在運用適當之控制措施，避免因人為疏失、蓄意或自然災害等風險，來確保本社之資訊資產能夠受到妥善之保護。
- 三、資訊安全之整體目標在確保資訊之機密性、完整性、正確性、即時性及可用性，防範本社之營運受到資安事件之衝擊。
- 四、資訊安全政策之適用範圍包括人員、軟體系統、硬體設備、機房及網路設施、資訊紀錄等五部分：
 - (一) 人員：本社經理人、聘雇員工、約聘員工及提供本社資訊服務之廠商人員。
 - (二) 軟體系統：本社各式主機、伺服器及個人電腦之作業系統及各式應用軟體、系統規劃與設計文件、使用與操作手冊。
 - (三) 硬體設備：本社各式主機、伺服器及個人電腦。
 - (四) 機房及網路設施：本社網路服務、空調、電力等。
 - (五) 資訊紀錄：本社系統資料庫及作業資料庫之各式記錄等。
- 五、本社為統籌資訊安全管理等事項之協調及推動，其幕僚作業，由資訊室負責。
- 六、本社就下列事項，訂定相關管理規範或實施計畫，並定期評估實施成效：
 - (一) 資訊安全管理組織推動及權責。
 - (二) 人員安全管理及教育訓練。
 - (三) 電腦系統安全管理。
 - (四) 網路安全管理。
 - (五) 系統存取控制。

附錄九十六之一

(六) 各式主機、伺服器及個人電腦之作業系統及各式應用軟體維護之安全管理。

(七) 資訊資產之安全管理。

(八) 實體環境及環境安全管理。

(九) 營運持續管理之安全之準則。

前項相關管理規範或實施計畫所需之細部作業程序及表單等，由各有關單位研擬，簽報單位主管核定後實施。

七、 資訊安全管理之分工原則：

(一) 資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由本社資訊室負責辦理。

(二) 資料及資訊系統之安全需求研議、使用管理及保護等事項，由各業務單位負責辦理。

(三) 資訊機密維護及資訊安全之稽核事項，由本社稽核單位辦理。

八、 本社同仁應遵守維護公務機密之相關法令規定；在職及離退職後，均不得洩漏所知悉之業務機密，或為不當之使用。

九、 為維業務正常運作，對資訊安全事件應建立緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，並向金融資安資訊分享分析中心(F-ISAC)通報，並聯繫檢警調單位協助偵查。

十、 本政策應以書面或其他方式告知本社同仁及提供本社資訊服務之廠商，以利共同遵守。若違反本社資訊安全相關規定，得依情節輕重予以處分或追究其民、刑事責任。

十一、 本政策應每年至少評估1次，或於發生重大變動時重新評估，以符合相關法令、技術及組織、營運之最新發展現況。

十二、 本政策經理事會通過後施行，修訂時亦同。