基隆二信資訊安全政策

113 年 10 月 24 日第 10 次理事會核定通過

第 一 條　為強化資訊安全管理，建立安全及可信賴之資訊作業，確保資料、系統、設備及網路之機密性、完整性及可用性並保障客戶權益，特訂定本政策，以作為本社實施各項資訊安全措施之依據。

第 二 條　本政策闡明本社員工應遵循之資訊安全政策，以及在資訊安全工作規劃、實踐與持續改進過程中所應扮演之角色與權責。範圍包括：

一、 組織與人員：所有員工、約聘雇人員、協力廠商及顧問等。

二、 資料文件：所有資料、文件、公文與報告等。

三、 軟體資訊資產：所有應用系統、工具程式、套裝軟體資料庫、作業系統等。

四、 硬體資訊資產：所有伺服器、個人電腦、儲存媒體、終端設備通訊線路等。

第 三 條　資訊安全管理之範圍應至少涵蓋下列事項：

一、 資訊安全管理組織及權責。

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。

六、 系統開發及維護之安全管理。

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。

十、 其他資訊安全管理事項。

第 四 條　為統籌本社資訊安全管理事項，應召集資訊安全管理會議，並由副總經理級以上人員擔任召集人及指派幕僚單位，負責執行與協調資訊安全會議相關之決議。

第 五 條　資訊安全應遵循之項目：

一、 所有本社擁有之資訊資產，在社內之資訊系統設備及網路資源上所處理、儲存或傳輸交換之資訊均歸屬本社財產，本社具有觀看、複製或取用之權利。

二、 本社所有員工、約聘雇人員、協力廠商及顧問，凡使用本社資訊以提供資訊服務或執行專案工作等，均有責任及義務保護其所取得或使用之資訊資產，以防止遭未經授權存取、擅改、破壞或不當揭露。

三、 本社各單位人員，對所負責業務而持有之資訊資產應負保管責任，確保重要資訊資產之機密性、完整性及可用性，防止其遭受意外或蓄意破壞、擅改、不當揭露或損失(包含實體或電子方式竊取)，以符合本社之營運利益並遵循相關法律及法規之要求。

四、 維護保障資訊安全為每位人員之義務，當認知有違資訊安全之情事，應予即時防制並進行通報。

五、 各項管理、行政及技術作業之發展、制訂及變更，應考量資訊安全之需求。

六、 各項作業中獲知之資訊，其資訊保護及保密責任不因工作變更而滅失。

七、 各項資訊資產之取存運用，包括電腦、網路設施及資訊系統等軟硬體之安裝、建置、發展、使用及維護，應參照相關的作業程序並獲得授權後方可執行。

八、 應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊

安全教育訓練及宣導，建立員工資訊安全認知，提升本社資訊安全水準及資訊安全管理能力。

九、 應應建立防病毒及防駭機制，保護資訊作業及相關資產，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為。

十、 為維護網路安全，防範電腦病毒之侵襲，應購買合法防毒軟體或關閉不必要之網路連線及服務，並定時更新相關病毒碼及掃毒引擎。

十一、對資訊安全事件應建立緊急通報機制，在發生資訊安全事件時，應依處理程序，立即向主管機關通報，並視業務需求訂定業務持續運作計畫，定期測試演練。

十二、資訊安全措施，應符合法律之規範與本政策要求。

第 六 條　本政策每年至少評估一次，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。

第 七 條　員工違反資訊安全相關規定者，其應負之資訊安全責任，依本社工作規則及相關規定辦理。

第 八 條　本政策如有未盡事宜，悉依有關法令及本社相關規定辦理。

第 九 條　本政策經理事會通過後施行，修正時亦同。