全國農業金庫資訊安全政策

112年4月26日第5屆第17次董事會通過
112年8月23日第5屆第21次董事會修正通過
115年8月26日第6屆第9次董事會修正通過

第一條 全國農業金庫（以下稱本公司）為落實資訊安全管理，採用「規劃、落實、檢查、行動」的管理模式，建立符合資訊安全管理國際標準要求之資訊安全管理制度，維持可靠的資訊系統環境，落實資訊安全管理並持續改善，以強化資訊安全管理，確保機密資訊之機密性、完整性與可用性，特訂定本政策。

第二條 本公司應依有關法令，考量業務需求，進行資訊安全風險評估，採行適當及充足之資訊安全措施，確保本公司資訊蒐集、處理、傳送、儲存之安全。

第三條 本政策適用於本公司各項資訊資產及所有資訊使用者，包含聘僱人員、派遣人員、委外廠商及其他經授權使用資訊資產之人員。

第四條 資訊安全之目標如下：

一、保護本公司資訊資產之機密性、完整性與可用性。

二、保護本公司客戶資訊，避免未經授權者的存取及修改。

三、建立資訊作業持續運作計畫，以於最短時間支援本公司業務持續運作。

第五條 資訊安全目標執行成果，應於每年十二月底前提報本公司管理審查會議。

前項管理審查會議之設置與權責規範授權總經理另訂之。

第六條 資訊安全涵蓋範圍如下：

一、資訊安全組織。

二、人力資源安全管理及資訊安全教育訓練。

三、資產管理。

四、存取控制管理。

五、密碼規則管理。

六、實體及環境安全管理。

七、運作安全管理。

八、通訊安全管理。

九、系統獲取、開發及維護。

十、供應商管理。

十一、資訊安全事故管理。

十二、業務持續營運管理。

十三、法規遵循性管理。

十四、其他資訊安全管理事項。

第七條 本公司應設置隸屬於總經理之資訊安全部，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備，並指派副總經理以上或職責相當之人擔任資訊安全長，綜理資訊安全政策推動及資源調度事務。

資訊安全部應每年依據法令、技術及業務之最新發展狀況評估檢視本政策之合宜性、適切性及有效性，以確保資訊安全。

第八條 本公司資訊安全長每年應向董事會報告前一年度資訊安全整體執行情形，並及時報告重大資安問題。

本公司資訊安全部人員，每年至少應接受十五小時以上資訊安全專業課程訓練或職能訓練；其他資訊從業人員則每年至少應接受六小時以上之資訊安全專業課程訓練或職能訓練。總公司、營業單位、財務保管單位及其他管理單位之人員，每年至少須接受三小時以上資訊安全宣導課程。

第九條 資訊安全部應辦理事項至少包括：

一、負責資訊安全制度之規劃、管理及執行，以控管資訊安全風險。

二、督導各單位落實資訊安全制度，並確保資通系統、服務及資訊之機密性、完整性與可用性。

三、建立資通安全防護、資通安全情資之評估因應與資通安全事件通報及應變相關機制。

四、每年應將前一年度資訊安全整體執行情形納入內部控制制度執行情形評估。

第十條 本公司聘僱人員、派遣人員、委外廠商等相關人員違反資訊安全相關規定者，應負資訊安全責任，並依相關人事規章或契約內容辦理。

第十一條 本政策未盡事宜悉依有關法令及本公司相關規定辦理。

第十二條 本政策經董事會通過後施行，修正時亦同。