

永豐金融控股股份有限公司
資訊安全政策辦法

非因應外規訂定
因應外規訂定

制定單位：資訊安全處

核准層級：董事會

第一條 為強化本公司及各子公司之資訊安全管理，建立安全及可信賴之資訊系統，確保資料、系統、設備及網路安全，提升同仁對資訊安全之認知，保障客戶權益，符合資訊安全相關規定，特訂定本政策辦法。

第二條 本政策辦法所稱之子公司，應依金融控股公司法第四條規定認定。

第三條 本政策辦法所稱的資訊安全，係指確保本公司及各子公司資訊處理之機密性、完整性與可用性，主要目的如下：

機密性(Confidentiality)：確保只有經授權的人才可以存取資訊。

完整性(Integrity)：保護資訊與處理方法的正確性與完整性。

可用性(Availability)：確保經授權的使用者在需要時，可以存取資訊及相關資產。

第四條 為有效推行資訊安全工作，應設置資訊安全委員會，其規程另訂之。

第五條 資訊安全涵蓋範圍如下：

- 一、資訊安全權責分工。
- 二、資訊安全教育訓練。
- 三、資訊系統安全管理。
- 四、網路安全管理。
- 五、應用系統存取管理。
- 六、應用系統開發及維護管理。
- 七、電腦資產管理。
- 八、系統環境安全管理。
- 九、資訊系統災害復原管理。
- 十、其他資訊安全管理事項。

前項第三款至第九款之作業，依據本公司「資訊管理準則」與「資訊設備與資源使用者準則」規定辦理。

第六條 資訊安全權責分工原則如下：

- 一、資訊安全政策辦法、計劃及技術規範之研議、建置及評估等事項，由資訊安全委員會召集人指定專人負責辦理。

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，由各應用系統經管單位負責辦理。

三、資訊安全風險管理制度之檢視及評估由風險管理處負責辦理。

四、資訊安全政策與管理制度適法性之檢視及評估由資訊安全委員會召集人指定專人負責辦理。

第七條 資訊安全教育應針對管理、業務及資訊等不同工作類別之需求，辦理資訊安全教育訓練及宣導，建立員工資訊安全認知與資訊安全管理能力，提升本公司資訊安全水準。

第八條 各單位如發生資訊安全事件，應立即依「緊急事件因應要點」辦理，並通報資訊安全委員會召集人指定專人進行因應處理，該指定專人應評估影響範圍、擬定因應計畫，並通報召集人進行必要決策與工作調度。

第十條 各子公司得視實際管理需求，依本政策辦法訂定該子公司應遵循之資訊安全相關規章，並報資訊安全委員會備查。

第十一條 本政策辦法如有未盡事宜，悉依主管機關相關法令與本公司相關規定辦理。

第十二條 本政策辦法經董事會核定後施行，修正時亦同。

中華民國一〇一年六月二十二日第四屆董事會一〇一年第六次會議通過

中華民國一〇一年十二月二十一日第四屆董事會一〇一第十二次會議修正通過

中華民國一〇二年六月二十一日第四屆董事會一〇二年第六次會議修正通過

中華民國一〇七年四月十七日修正(依金控內部規章制定及公告規則第三條及第六屆董事會一〇七年第三次會議修正通過)

中華民國一〇七年九月二十一日第六屆董事會一〇七年第九次會議修正通過

中華民國一〇九年六月十九日第七屆董事會一〇九年第三次會議修正通過