

# 資訊安全政策

- 第一條 國票金融控股公司(以下簡稱本公司)為強化資訊安全管理，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，符合資訊安全相關規定，特訂定本政策。
- 第二條 資訊安全之定義，係指確保本公司資訊處理之正確性，作業人員所使用之電腦軟體、硬體、週邊及網路系統之可靠性，並確保上述資源免受干擾、破壞、入侵之行為或企圖。
- 第三條 資訊安全之目標，係為確保本公司資訊的合法存取，於可能遭受外力入侵時，亦能提供完整、未中斷之資訊系統運作；於事故發生時，得於必要之應變處置後，能在最短時間內回復正常運作，以降低該事故可能帶來之損害。資訊安全之範圍如下：
- 資訊安全分工組織及職掌。
  - 人員管理及資訊安全教育訓練。
  - 資訊系統發展及維護安全管理。
  - 系統與檔案安全管理。
  - 電腦設備運轉安全管理。
  - 網路安全管理。
  - 資訊資產安全管理。
  - 系統存取控制管理。
  - 實體及環境安全管理。
  - 資訊作業安全及資料保密管理。
- 第四條 前條之作業，依據本公司「電腦資訊安全維護管制及作業要點」、「資訊業務規章」、「電腦主機及伺服器安全管理作業要點」、「網站管理作業要點」、「電腦機房緊急應變計畫」規定辦理。
- 第五條 為強化員工資安意識，應於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。
- 第六條 為防範電腦病毒或惡意程式入侵，應購買合法防毒軟體，並定時更新相關病毒碼及掃毒引擎。
- 第七條 員工應簽署保密切結書，遵守資訊安全保密協定，接受適當之教育訓練或宣導，告知內部人員遵循資訊安全相關規範。
- 第八條 辦理公司業務委外作業時，應明定廠商之資訊安全責任及保密規定，並載明於契約。
- 第九條 應建立資訊安全防禦機制並定期辦理下列資訊安全檢視作業，以改善並提升資訊安全防護能力。
- 一、資訊架構檢視。
  - 二、網路活動檢視。

三、網路設備、伺服器及終端設備等檢測。

四、網站安全檢測。

五、安全設定檢視。

第十條 各單位如發生資通安全事件，應即通報資訊處處理，並由資訊處依相關規定通報主管機關，並採取適當處理措施，以控制資安事件影響之範圍。

第十一條 本政策至少每年經「資訊安全管理單位」評估一次，以符合相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

第十二條 本政策未盡事宜，悉依有關法令及本公司相關規定辦理。

第十三條 本政策經董事會通過後實施；修正時亦同。

規章衍歷：民國一〇八年十月二十三日第六屆董事會第二十次會議通過。