國泰證券投資顧問股份有限公司
資訊安全政策

106 年 11 月 3 日訂定
110 年 11 月 8 日修訂
權責單位：行政管理部

主旨

第一條 為強化國泰證券投資顧問股份有限公司（以下簡稱本公司）之資訊安全管理，建立安全及可信賴之資訊作業環境，確保資訊資產之機密性、完整性、可用性及適法性，避免遭受內、外部蓄意或意外之威脅，並提升同仁對資訊安全之認知，以保障本公司所有人員、客戶與本公司之權益，特訂定本公司資訊安全政策（以下簡稱本政策）。

政策聲明

第二條 本公司資訊安全管理之政策聲明如下：

一、 本公司資訊安全管理，應依循本公司適用之相關法令、主管機關規定及本政策之規定辦理。

二、 本公司資訊資產嚴禁未經授權存取與揭露。

三、 資訊系統建置應考量有效之資訊安全措施，以降低內部網路及電腦主機系統遭受外部駭客或內部人士之入侵攻擊或未經授權存取等威脅風險。

四、 針對資訊系統，探討系統中斷可能造成之營運中斷風險，進而發展應變、備援或復原計畫，並定期進行演練。

五、 本公司所有人員（以下含約聘雇人員、工讀生、派遣人員）均有責任及義務保護其所取得或使用之本公司資訊資產，防止未經授權存取、擅改、破壞或不當揭露，並應遵守維護公務機密之相關法令規定，於在職及離退職後，均不得洩漏所知悉之業務機密，或為不當之使用。

六、 本公司有權管理歸屬於本公司之資訊資產，包含但不限於在本公司資訊資產或以本公司名義使用網路資源上所處理、儲存或傳輸交換之資訊。

七、 資訊業務委託合約，應規範下列事項：

1. 委託作業事項範圍及受委託機構之權責。
2. 受託人員應善盡責任保護本公司資訊資產，未經授權不得任意揭露、存取、擅改、破壞。
3. 受託人員應遵守本政策與相關管理規範，對於有發生資訊安全事件、弱點及違反本公司資訊安全政策與管理規範之虞者，應隨時保持警戒，並立即通報本公司資安權責單位。
4. 保密條款及查核條款。
5. 合約終止與解約條款。
6. 罰則及損害賠償條款。

7. 其他必要事項。

八、 本公司應以書面或其他方式將本政策或政策聲明告知同仁、與本公司資訊安全有利害關係之個人或團體及提供資訊服務之廠商等，以利共同遵守。若違反資訊安全相關規定，得依情節輕重予以處分或追究其民、刑事責任。

適用對象及範圍

第三條 本政策適用對象為本公司所有人員及其他得接觸本公司業務相關資訊之合作夥伴、委託廠商（含顧問）等。

本政策適用範圍如下（以下合稱資訊資產）：

一、 本公司所有電子資料與紙本文件。

二、 本公司所有主機、伺服器、個人電腦、終端設備、通訊線路，以及與前述設備相關或是與本公司資訊系統相連等之硬體資訊資產。

三、 本公司所有存放硬體資訊資產之實體環境。

四、 本公司所有應用系統，以及與前述應用系統相關或是與本公司資訊系統相連等之軟體資訊資產。

五、 其他本公司所有資訊資產，或其他本公司未實際所有，但基於合約、法律及法規所賦予之責任而可支配之資訊資產。

用詞定義

第四條 本政策相關用詞定義如下：

一、 資訊：係指以任何型態顯示及以任何媒體（含紙張）紀錄或儲存之未經處理之原始資料、經處理之資訊、及轉換提升後之知識等。

二、 資訊安全：目的在確保資訊的機密性、完整性、可用性、私密性及合法性，使資訊能安全地、正確地、適切地及可靠地被運用在達成本公司經營目標之規劃、執行、管理及相關作為上，運用適當之控制措施來確保資訊資產受到妥善之保護，避免因人為疏失、蓄意或自然災害等風險。

資訊安全管理

第五條 本公司之資訊安全目標如下：

一、 確保本公司資訊作業均符合相關法令規定要求。

二、 確保本公司資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。

三、 確保本公司資訊作業管理之完整，避免未經授權之修改。

四、 確保本公司資訊作業之持續運作。

五、 確保本政策適用對象對於資訊安全之認知與遵行。

第六條 本公司之資訊安全控制措施如下：

一、 取得管理階層承諾及支持，建立資訊安全管理制度，定期檢視並適時更新資訊

安全管理制度之文件，管理留存相關紀錄。定期鑑別及處理資訊安全風險、量測資訊安全指標，以持續維持資訊安全管理制度及管控程序實施之有效性。

二、 成立資訊安全管理組織，督導資訊安全管理制度之運作，鑑別資訊安全管理制度之內、外部議題及利害相關團體對本公司資訊安全之要求與期望。

三、 本公司人員皆應接受與職務相關之資訊安全教育訓練，並熟悉本身工作中之資訊安全職責；對於與本公司具業務往來之廠商及其員工、臨時雇員、訪客應審核其對本公司資訊資產存取、擁有、保管或使用之必要並責予保護之義務。

四、 定期清查本公司資訊資產並進行適當分類分級。

五、 工作分派應考量職能分工，職務責任範圍與作業權限應予區分，並建立權限審核及檢視機制，以避免資訊或服務遭未經授權修改或誤用。

六、 確保工作區域場所之安全，以防範資訊資產遭竊取或毀損。

七、 遵循職責相關資訊作業處理程序，以正確並安全地管理資訊系統。

八、 落實通訊安全管理，以保護網路連線之安全。

九、 資訊系統或程式建置、開發及變更應依循本公司相關程序辦理，並納入資訊安全相關議題。

十、 善盡對供應商監督與管理之責任。

十一、 隨時注意是否有發生資訊安全事件、安全弱點及違反安全政策與規範之虞之情事，並依程序進行通報。

十二、 依業務需求訂定資訊作業營運持續計畫，並定期測試演練。

十三、 遵循內外部相關法令規定，建立應有之管控程序，定期執行資訊安全查核作業。

第七條 本政策每年至少審查一次，以符合相關法令規定及資訊業務最新發展現況，並於必要時修正之。

第八條 本政策經本公司董事會核定後實施，修正時亦同。