國泰金融控股股份有限公司資訊安全政策

96.04.27 訂定
102.02.06 修正
107.03.15 修正
108.03.21 修正
110.08.19 修正
111.05.13 修正
112.05.11 修正
114.04.23 修正
114.08.15 修正

權責單位：資訊安全處

第一條　目的

為強化國泰金融控股股份有限公司(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、完整性及可用性，並提升同仁對資訊安全之認知，以保障員工、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)。

第二條　政策聲明

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，應依個人資料保護法、金融控股公司法、金融控股公司及銀行業內部控制及稽核制度實施辦法、金融控股公司及其子公司自律規範等相關法令、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之存取、揭露與破壞，確保資訊於整個生命週期內維持適當之安全控制措施，以防範資訊安全事件。

三、資訊系統建置與使用第三方提供之雲端服務應考量有效之資訊安全措施，以降低網路及電腦主機系統遭受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、本公司所有員工(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。

五、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。

六、資訊業務委託合約，應規範下列事項：

(一) 委託作業事項範圍及受委託機構之權責。

(二) 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。

(三) 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，並立即通報本公司相關業務負責單位以及資訊安全處。

(四) 保密條款及查核條款。

(五) 合約終止與解約條款。

(六) 罰則及損害賠償條款。

(七) 其他必要事項。

第三條　適用對象及範圍

本政策適用對象為本公司所有員工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、雲端服務業者)等。

本政策適用範圍如下(以下合稱資訊資產)：

一、本公司所有資料與文件。

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、雲端服務，以及與前述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。

第四條　用詞定義

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、及轉換提昇後之知識等。

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。

三、雲端服務：係指本公司為進行運算、儲存、備份等作業，而向雲端服務業者所承租之服務，包括但不限於網路設備、伺服器、儲存空間、資安設備、系統軟體、應用程式、分析與計算等資源等；非向外部雲端服務業者承租者，則依本政策其他相關規定辦理。

四、雲端服務業者:指以租借方式提供個人或企業得承租其網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源之協力廠商。

第五條　資訊安全管理單位與分工

基於業務推動與資訊安全控管平衡性，並提升對資訊安全之重視，應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。本公司應指派副總經理以上或職責相當之人擔任(兼任)資訊安全長，綜理資訊安全政策推動及資源調度事務，並應設置具職權行使獨立性之資訊安全專責單位，獨立於資訊單位外，以及指派協理或職責相當以上人員擔任(兼任)資訊安全專責單位主管，且不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當之資安專責人員。

資訊安全專責單位負責規劃、監控、及執行資訊安全管理作業，每年應

將前一年度資訊安全整體執行情形提報董事會。

第六條 為維持資訊安全管理有效運作，本公司資訊管理單位與資訊安全專責單位依循第一道及第二道防線畫分為原則。

資訊安全第一道防線權責單位為資訊處及涉及資訊開發、資訊維運之相關單位(以下統稱資訊管理單位)，資訊開發包含資訊系統或資訊安全機制於開發或導入階段的規劃與設計等，資訊維運包含資訊系統或資訊安全機制於管理階段的建置、維運、監控、事件通報與處理等，或依實務需求由資訊管理單位委由子公司代為辦理。

資訊安全第二道防線權責單位為資訊安全處，主要負責資訊安全策略與藍圖規劃、推動資訊安全政策、資訊安全執行情形的監控管理、資訊安全缺失與事件的改善追蹤、以及資訊安全教育訓練與宣導等。

資訊安全之各項作業若委由子公司代為管理，子公司之資訊安全控管較本公司之要求更為嚴格者，應以子公司之標準進行管理。

若本公司員工兼任子公司職務，或子公司員工兼任本公司職務者，該員工應以所使用資訊資產之資訊安全控管較為嚴格者之標準進行管理。

第七條 資訊安全治理架構

為有效推展本公司整體資訊安全，並督導子公司之資訊安全執行情形，應設置「資訊安全委員會」：

一、召集人及成員：

由本公司資訊安全最高主管擔任召集人，並得設立副召集人。另邀請總經理列席指導，執行祕書由資訊安全處部室主管擔任。委員會成員為本公司及子公司之資訊安全與資訊單位最高主管。無資訊或資訊安全專責單位之子公司，由指定的專責人員擔任，並得邀請本公司相關單位主管參與。

二、會議召集：

每半年召開一次會議，並得視需要召開臨時會議。

三、組織任務：

(一) 本公司資訊安全政策之擬議。

(二) 本公司及子公司資訊安全管理制度之推展。

(三) 本公司及子公司資訊安全意識之提升及教育訓練計畫之擬議。

(四) 本公司及子公司整體資訊安全執行情形之檢視督導。

(五) 跨子公司重大資訊安全專案之討論與決策。

第八條 為推行資訊安全作業，有效進行橫向溝通聯繫，並達成本公司及子公司整體資訊安全管理的一致性，應設置「資訊安全聯繫會」：

一、召集人及成員：

由本公司資訊安全最高主管擔任召集人，並得設立副召集人，執行祕書由資訊安全處部室主管擔任。聯繫會成員為本公司及子公司之資訊安全最高主管、資訊安全各級主管，以及資訊安全人員，並得邀請資訊或業務相關單位主管參與。

二、會議召集：

每月召開一次會議，並得視需要召開臨時會議。

三、組織任務：

(一) 本公司及子公司資訊安全資安藍圖及基本管控需求項目規劃討論。

(二) 本公司及子公司資訊安全管理制度之適法性與合宜性檢視討論。

(三) 本公司及子公司資訊安全執行情形之彙整報告。

(四) 本公司及子公司資訊安全專案之討論與規劃。

(五) 本公司及子公司資訊安全相關事務的溝通協調。

第九條 資訊安全事件管理原則

本公司所有員工發現或接獲外部單位通報疑似資安事件、其他可能違

反資訊安全政策與相關規範之情形或面臨外部之威脅時，應隨時保持警戒，並依程序進行通報。

若發生重大資訊安全事件，本公司將向可能受影響的利害關係人保持透明溝通，說明處置作為與預防措施，以降低風險再發生。

第十條　政策評估

本政策應視政府法令、技術及業務等最新發展現況做必要之修改，並每年定期評估其適切性。

評估結果應作為持續改善資訊安全管理制度之依據，以因應資安風險之變化，確保資訊安全機制能有效保護組織資產。

第十一條　施行日期

本政策經董事會決議通過後施行，修正或廢止時亦同。