國票金融控股股份有限公司
個人資料檔案安全維護辦法

第一章 總則

第 一 條 本辦法係依據個人資料保護法(以下稱本法)及金融監督管理委員會(以下稱金管會)指定非公務機關個人資料檔案安全維護辦法訂定。

第 二 條 本辦法訂定之目的與宗旨係為規範個人資料之蒐集、處理及利用，防止個人資料被竊取、竄改、毀損、滅失或洩漏，落實個人資料檔案安全維護與管理，進而降低個人資料損害之發生，並維護當事人之權益。

第二章 個人資料保護之規劃

第 三 條 本公司應依業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，以規劃、訂定、修正與執行個人資料檔案安全維護計畫及業務終止後個人資料處理方法。

第 四 條 本公司應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本辦法之範圍。

第 五 條 本公司應依前條界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據 風險評估之結果，訂定適當之管理機制。

第 六 條 本公司為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故(以下簡稱事故)，應訂定下列應變、通報及預防機制：

一、事故發生後應採取之各類措施，包括：

(一)控制當事人損害之方式。

(二)查明事故後通知當事人之適當方式。

(三)應通知當事人事故事實、所為因應措施及諮詢服務專線等內容。

二、事故發生後應受通報之對象及其通報方式。

三、事故發生後，其矯正預防措施之研議機制。

本公司遇有重大個人資料事故時，應依附件格式於七十二小時內通報金管會。但於其他法令另有規定時，並應依各該法

令之規定辦理。前項所研議之矯正預防措施，並應經公正、獨立且取得相關公認認證資格之專家，進行整體診斷及檢視。

前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及本公司正常營運或大量當事人權益之情形。

第 七 條　本公司應定期對所屬人員，施以個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。

第三章　個人資料之管理程序及措施

第 八 條　本公司應就下列事項，訂定個人資料之管理程序：

一、蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。其經當事人書面同意者，並應確保符合本法第六條第二項準用第七條第一項、第二項及第四項之規定。

二、檢視個人資料之蒐集、處理，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。

三、檢視一般個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條之規定。

四、檢視一般個人資料之利用，是否符合本法第二十條規定蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合本法 第七條之規定。

五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。

七、進行個人資料國際傳輸前，檢視是否受金管會限制並遵循之。

八、當事人行使本法第三條所定權利之相關事項：

(一)當事人身分之確認。

(二)提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。

(三)對當事人請求之審查方式，並遵守本法有關處理期限之規定。

(四)有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。

九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。

十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定刪除、停止處理或利用。

第 九 條　本公司為維護所保有個人資料之安全，應採取下列資料安全管理措施：

一、訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用 時，應採取防範資料洩漏之適當措施。

二、針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

三、作業過程有備份個人資料之需要時，對備份資料予以適當 保護。

第 十 條　本公司如有提供電子商務服務系統，應採取下列資訊安全措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、應用系統於開發、上線、維護等各階段軟體驗證與確認程 序。

五、個人資料檔案及資料庫之存取控制與保護監控措施。

六、防止外部網路入侵對策。

七、非法或異常使用行為之監控與因應機制。

前項所稱電子商務，係指透過網際網路進行有關商品或服務之廣 告、行銷、供應、訂購或遞送等各項商業交易活動。

第一項第六款、第七款所定措施，應定期演練及檢討改善。

第十一條　公司保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採 取下列設備安全管理措施：

一、實施適宜之存取管制。

二、訂定妥善保管媒介物之方式。

三、依媒介物之特性及其環境，建置適當之保護設備或技術。

第十二條　本公司為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人 員約定保密義務。

第四章　個人資料之安全稽核、紀錄保存及持續改善機制

第十三條　本公司為確保本辦法之落實，應依業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制；如依法令規 定應建立內部控制及稽核制度時，並應將相關機制列入內部控制及稽核項目。

第十四條　本公司執行本辦法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。

本公司依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

一、刪除、停止處理或利用之方法、時間。

二、將刪除、停止處理或利用之個人資料移轉其他對象者，其 移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

第十五條　為持續改善個人資料安全維護，本公司所屬個人資料管理單位或人員，應定期提出相關自我評估報告，並訂定下列機制：

一、檢視、修訂本辦法相關個人資料保護事項。

二、針對評估報告中有違反法令之虞者，規劃、執行改善及預 防措施。

前項自我評估報告，並授權由總經理核定。

第五章　附則

第十六條　本辦法未盡事宜，悉依相關法規或本公司相關規定辦理，有關個人資料保護事務之執行及各項作業要點之訂定或修正，均授權總經理核定及處理。

第十七條 本辦法經董事會核定後施行，修正時亦同。

規章衍歷：

中華民國一〇三年二月十日第四屆董事會第五次臨時會通過。

中華民國一〇四年八月二十六日第五屆董事會第十次會議修正通過。

中華民國一〇五年八月二十四日第五屆董事會第十八次會議修正通過。

中華民國一一一年五月十八日第七屆董事會第二十二次會議修正通過。

個人資料檔案安全維護辦法第六條附件

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>非公務機關名稱
_____

通報機關
_____</td><td colspan="2">通報時間： 年 月 日 時 分通報人： 簽名(蓋章)
職稱：電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個資 _____ 筆 □特種個資 筆
_____</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後 72 小時通報本會</td><td colspan="2">□是 □否，理由</td></tr>
</table>

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註2：上開72小時通報本會，例假日均納入時效計算。