國泰金融控股股份有限公司個人資料檔案安全維護計畫暨業務終止後個人資料處理方法

103.03.14 訂定
103.07.31 修正
權責單位：風險管理處

壹、依據

依據金融監督管理委員會發布之「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第三條規定辦理。

貳、目的

訂定本公司「個人資料檔案安全維護計畫暨業務終止後個人資料處理方法」（以下簡稱本計畫），以加強管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，確保個人資料之安全維護。

參、本計畫內容

一、 個人資料管理組織

1.成立「個人資料管理委員會」(後稱委員會)，負責本計畫之執行、督導及管理。

2.由總經理擔任主任委員，依「國泰金融控股股份有限公司個人資料管理委員會權責及組織辦法」召集委員會行使職權。

二、 個人資料檔案盤點及風險評估

1. 由各部處法遵人員或部室主管指派之人員，定期(每年至少一次)執行下列事項，並由各部處主管審核執行結果後，自行保留並送風險管理處備存：

   (1) 更新個人資料檔案清冊

   (2) 更新企業資訊流概覽圖(BIF)

   (3)填寫「個人資料管理衝擊分析表」(PIA)

2. 由風險管理處將各部處 PIA 填寫結果，列入風險評估項目，並於考量資產權值、弱點權值、威脅權值及計算風險值後，送交委員會審議。

3. 風險管理處應就高風險項目，與相關部處(下稱「改善單位」)研議擬訂風險處理計畫，以降低風險至可接受水準。

4. 改善單位應依前項風險處理計畫之改善方式及改善期限，進行改善作

業。

三、 個人資料安全事件管理

1. 依「國泰金融控股股份有限公司個人資料侵害事件管理辦法」及相關規章辦法規定，執行個人資料侵害事件之通報、應變、預防及強化作業。
2. 定期檢視個人資料侵害事件時之通報、應變、預防及強化機制，俾於個人資料侵害事件發生時，能夠及時掌握事件狀況，以降低事件所造成之損害。
3. 若有危及本公司正常營運或大量當事人權益之重大個人資料安全事件，應即通報金融監督管理委員會。

四、 個人資料保護之教育訓練

1. 定期(每年至少一次)對公司正式及約聘員工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。
2. 由風險管理處製作個人資料保護教材，內容包含：
   (1)新進員工認知宣導及測驗。
   (2)在職員工定期教育訓練及測驗。
   (3)不定期提供各部處宣導教材，並由各部處執行訓練。
3. 各部處應配合風險管理處之規畫執行教育訓練，除自行保留測驗結果或受訓紀錄外，並應提供風險管理處存查。

五、 個人資料管理查核

定期(每年至少辦理一次)查核本計畫之落實狀況、內部控制事項之落實情形及各部處盤點之個人資料檔案現況。

六、 個人資料管理事項

1. 應確保個人資料之蒐集、處理及利用之特定目的、必要條件、告知事項、正確性、及特定目的消失或期限屆滿時之刪除、停止處理或利用，符合「個人資料保護法」第六條、第七條、第八條、第九條、第十一條、第十九條及第二十條之規定。
2. 應依「國泰金融控股股份有限公司個人資料蒐集、處理與利用管理辦

法」、「國泰金融控股股份有限公司個人資料當事人權利行使管理辦法」及相關規章辦法規定，執行個人資料檔案管理事項。

3. 應於當事人表示拒絕行銷時，立即通知各子公司停止利用其個人資料進行行銷。
4. 如有進行個人資料國際傳輸時，應遵循相關法令及金融監督管理委員會之限制。
5. 確保提供當事人權利之行使方式，符合個人資料保護法第三條之規定。

七、 個人資料安全、人員及設備管理

1. 各系統設備管理單位於系統設備移交他單位使用或報廢前，應先移除儲存資料。儲存媒體之銷毀，應依媒體特性進行銷毀，以確保報廢媒體已無法讀取或繼續使用。
2. 各單位對內（外）以人員、(電子)郵件等各種方式所傳遞之資料，若資料內容含個人資料時，應依本公司相關規章辦法規定進行資料遮蔽，若無法進行遮蔽，應採取其他保護措施(如專人親送或電子郵件加密)，作為補償性控制。
3. 電腦資訊設備及儲存媒體之安全管理設備，應設有門禁管理、錄影監控設備或以上鎖等方式管控。
4. 對於接觸個人資料之人員，應設定其使用管理權限，並同步保留接觸、使用資料等之紀錄。

八、 個人資料之紀錄保存

執行本計畫所定各種個人資料保護機制、程序、措施及依個人資料保護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，應留存軌跡資料或相關證據至少五年，但法令另有規定或契約另有約定者，不在此限。

九、 業務終止後個人資料處理方法

個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

肆、 本計畫執行情形之自我評估報告

風險管理處應定期檢視、修訂本計畫相關之個人資料保護事項，並於委員會定期會議中，提出報告，如有違反法令之虞者，並應規劃、執行改善及預防措施。前述報告，應於提報委員會後由總經理核定之。

伍、 本計畫施行與授權修正

本計畫經董事會核准後施行，並授權總經理修正之。