凱基金融控股股份有限公司
個人資料檔案安全維護計畫及業務終止後個人資料處理要點

管轄單位：法令遵循處
初訂發布日：102.12.27
修正發布日：114.3.10

第 一 章　總則

一、 本計畫及處理要點依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及本公司個人資料保護管理政策訂定之。

二、 本計畫及處理要點用詞定義如下：

(一) 當事人：指個人資料之本人。

(二) 個人資料安全事故：指內部或外部通報發現之事件中，依其發生之原因及影響，涉及個人資料之竊取、竄改、毀損、滅失、洩漏或其他侵害當事人權益者。

(三) 重大個人資料安全事故：指個人資料安全事故之發生，將危及本公司正常營運或大量當事人權益之情形。

(四) 事故責任單位：指針對個人資料安全事故之發生原因應負責之單位。

(五) 特種個人資料：指個人資料保護法第六條第一項規定之有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

三、 本公司個人資料管理之範圍，包含全體從業人員與合作廠商，因執行業務、專案與內部行政作業，所涉及個人資料之蒐集、處理及利用等活動。

四、 本公司個人資料管理之目標如下：

(一) 符合相關法令及主管機關規範，建立適當之個人資料保護制度，確保個人資料妥善管理。

(二) 有關個人資料之蒐集、處理及利用之作業流程，應防止個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他不合理之利用。

(三) 善盡本公司善良管理人之注意責任，以建立當事人信任基礎並維護當事人權益。

第 二 章　個人資料保護管理組織

五、 有關本公司個人資料保護管理制度之審查與監督、各單位間之協調與配合、各項資源之整合與運用、及其他個人資料保護管理事項之審議與推動，應陳請總經理核定之。

六、 本公司應設個人資料保護核心小組(以下簡稱「核心小組」)，由各單位指派代表人員組成。核心小組應負責評估、規劃及執行本公司個人資料保護管理制度及相關作業、各單位間之協調與配合，以及本計畫及處理要點所定應由核心小組辦理之個人資料保護管理事項。

法令遵循處為核心小組之事務單位，負責召開及主持核心小組會議，並綜整前項有關核心小組應辦理之事項。

各單位核心小組成員為所屬單位就個人資料保護管理事項之聯絡窗口，除參與核心小組會議反映相關問題及提出建議外，並應負責追蹤所屬單位就個人資料保護管理事項之執行。

第 三 章　界定個人資料之範圍

七、 為執行個人資料管理作業，資安單位應對各單位個人電腦中之個人資料擬定掃描計畫並執行之，各單位將個人電腦個人資料掃描處理結果納入個人資料相關業務流程識別及個人資料盤點作業內，以界定個人資料之範圍。

八、 前點之作業，應依下列程序為之：

(一) 各單位進行與個人資料相關業務流程識別作業，辨識含有個人資料之業務流程，並根據識別結果填具於「個人資料流程識別清單」(附件一)。

(二) 各單位根據「個人資料流程識別清單」，對含有個人資料之檔案進行盤點，並填具「個人資料盤點表」(附件二)。

前項「個人資料流程識別清單」及「個人資料盤點表」，應由各單位指派合適之人員填寫，經單位主管簽核後送核心小組。

九、 各單位應定期彙整及維護其「個人資料流程識別清單」、「個人資料盤點表」，並送交核心小組。

各單位遇有業務流程或個人資料檔案新增、廢止、異動（如業務流程或個人資料檔案內容調整或管理人員異動）之情事，應及時更新調整其「個人資料流程識別清單」及「個人資料盤點表」，並送交核心小組。

十、 本公司應配合第四章之風險評估作業頻率，每年至少執行一次業務流程識別及個人資料盤點作業。

核心小組如遇本公司組織變更、作業流程變更、個人資料檔案重要異動或發生重大個人資料保護事故等，得規劃針對特定範圍內之個人資料流程進行業務流程識別及個人資料盤點，交由相關單位執行之。

第 四 章　個人資料之風險評估及管理機制

十一、 各單位於完成個人資料範圍之界定後，應進行風險評估作業，每年至少一次。

十二、 前點之作業，應依下列程序為之：

(一) 各單位應就已識別之業務流程分別進行適法性分析及流程衝擊分析，並將分析結果分別記錄於「適法性分析表」(附件三)及「個人資料流程衝擊分析表」(附件四)。

(二) 各單位完成流程衝擊分析後，應進行風險評估作業，參考「風險情境表」(附件五)對應各業務流程適用之風險情境，計算各項業務流程對應之風險值，填寫於「個人資料流程作業風險評估表」

(附件六)，並據以擬訂「個人資料管理風險處理計畫」(附件七)。

前項「適法性分析表」、「個人資料流程衝擊分析表」、「個人資料流程作業風險評估表」及「個人資料管理風險處理計畫」，應由各單位指派合適之人員填寫，經單位主管簽核。

十三、 核心小組事務單位應就各單位完成之「個人資料流程作業風險評估表」進行風險排序，依據風險衝擊程度、風險值大小與可接受成本及分配資源，先行評估本公司可接受風險，針對超出可接受風險值之個人資料風險項目提出風險處理措施之建議，並據以撰寫「個人資料管理風險自我評估報告」初稿，提交核心小組討論後陳請總經理核定。

十四、 如遇本公司組織變更、作業流程變更、個人資料檔案重要異動或發生重大個人資料保護事故等，核心小組得規劃針對特定範圍內之個人資料流程進行風險評估，交由相關單位執行之。

十五、 有關本章所定之風險評估作業執行細節，應參照「個人資料風險評估與處理程序說明」(附件八)辦理。

第 五 章 個人資料安全事故之通報、應變及預防機制

十六、 本公司各單位人員，發現疑似個人資料安全事故時，應立即通知該單位核心小組成員辨識是否為個人資料安全事故。如經確認為個人資料安全事故，該單位應立即採取適當之應變措施，並填寫「個人資料安全事故通報單」(附件九)通報法令遵循處。法令遵循處接獲通報後，應召開核心小組會議辨識事故責任單位並協同實施應變措施。

個人資料安全事故如構成重大偶發事件者，應逕依「重大偶發事件應變作業辦法」辦理。

十七、 事故責任單位及相關單位應就個人資料安全事故依指示及視事件性質採取適當之應變措施，並應保存處理過程中之所有分析與紀錄。

核心小組應協同查明事故之原因及影響，並協調相關單位採取應變措施，防止事故擴大，減少因事故可能產生之損失。

前二項之應變措施得包含但不限於下列事項：

(一) 中斷入侵或洩漏途徑。
(二) 啟動備援程序或替代方案。
(三) 事故原因初步分析。
(四) 評估受侵害個人資料類別及數量。
(五) 檢視防護及監測設施功能。
(六) 記錄事故經過。
(七) 內部調查完成前保存相關證據。
(八) 解決或修復方案。
(九) 通知保有相同資料之其他單位。
(十) 洽商專業人員協助或進駐處理。
(十一) 涉及刑事責任者，移請檢警鑑識或調查。
(十二) 發布內部注意事項、外部新聞稿、網站公告及通知當事人或主

管機關。

十八、 個人資料安全事故查明後，應由事故責任單位諮詢核心小組事務單位，並報請總經理同意後，以適當方式通知當事人，告知個人資料被侵害之事實、本公司所為因應措施並提供諮詢服務專線。

前項通知得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得而知之方式為之，但應留存相關紀錄。若所需費用過鉅，亦得以網際網路、新聞稿或其他適當方式公開為之。

十九、 核心小組事務單位應彙整個人資料安全事故之完整資料及證據並追蹤其處理情形，並視情節之重大性，向總經理報告；其屬重大個人資料安全事故者，應依附件格式(附件十)於七十二小時內通報主管機關。

二十、 個人資料安全事故排除後，核心小組事務單位得視情況召集相關單位或人員進行事後檢討會議，針對事故之原因進行分析，並研議相關矯正預防措施，陳請經總經理核定後實施，以避免事故重複發生，或預防潛在事故發生。

如遇有重大個人資料安全事故者，第一項之矯正預防措施應委由公正、獨立且取得公認認證資格之專家，進行整體診斷及檢視。

第 六 章 個人資料蒐集、處理及利用之內部管理程序

二十一、各單位因執行業務所需，所進行個人資料之蒐集、處理及利用，應遵守以下原則：

(一) 蒐集、處理、利用個人資料時，必須尊重當事人權益。
(二) 採取誠實及信用之方法，不得刻意隱瞞當事人。
(三) 不得逾越特定目的之必要範圍。
(四) 應與蒐集目的具有正當合理的關聯。
(五) 蒐集、處理、利用之個人資料應以符合特定目的必要範圍內之最少資料欄位為原則。

二十二、各單位如因特殊需求須蒐集、處理或利用特種個人資料時，應符合相關法令之規定。

二十三、各單位直接向當事人蒐集其個人資料時，應依個人資料保護法第八條第一項履行告知義務。但有個人資料保護法第八條第二項情形者，不在此限。

前項告知之方式得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得而知之方式為之，並應留存相關資料以備查驗。

若當事人為無行為能力人、限制行為能力人或受輔助宣告人，告知對象及於其法定代理人、監護人或輔助人。

二十四、本公司所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知資料來源及個人資料保護法第八條第一項第一款至第五款所列事項。但有個人資料保護法第九條第二項情形者，不在此限。

二十五、個人資料之蒐集或處理，除特種個人資料外，應有特定目的，並符合下列之情形之一：

(一) 法律明文規定。

(二) 與當事人有契約或類似契約的關係，且已採取適當之安全措施。

(三) 當事人自行公開或其他已合法公開的個人資料。

(四) 經當事人同意。

(五) 為增進公共利益所必要。

(六) 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用顯有更值得保護之重大利益者，不在此限。

(七) 對當事人權益無侵害。

本公司知悉或經當事人通知依前項第六款但書規定禁止對該資料之處理或利用時，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。

二十六、個人資料如有下列情形之一者，得為特定目的外之利用：

(一) 法律明文規定。

(二) 為增進公共利益所必要。

(三) 為免除當事人的生命、身體、自由或財產上的危險。

(四) 為防止他人權益的重大危害。

(五) 經當事人同意。

(六) 有利於當事人權益。

二十七、個人資料若為行銷目的利用時，必須符合以下規範：

(一) 若當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

(二) 首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

二十八、本公司應就當事人就其個人資料權利之行使，訂定相關程序據以執行。

二十九、各單位受理各項業務，除應詳實核對個人資料外，若有依法留存證件影本者，應加註限制使用目的和範圍，以防杜當事人證件遭不法利用。

個人資料正確性有爭議者，除因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議外，各單位應主動或依當事人之請求停止處理或利用。

各單位受理當事人依個人資料保護法第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

各單位若發現曾提供錯誤或非最新之個人資訊予外部單位時，應主動通知外部單位，避免使用錯誤資訊而影響當事人權益。

三十、 個人資料之保存期限以五年為原則，但相關法令另有規定、本公司依執行業務之需要訂有保存期限、或依個別契約另有約定者，不在此限。

如因業務需求而有延長保留期限之理由（如事後稽核、比對或證明之需要），亦應充分考慮其保管成本，並落實資料保存之安全維護措施。

各項業務終止後個人資料之處理或涉及資料之刪除或銷毀，應留存相

關紀錄。

三十一、為確保個人資料傳輸至國（境）外時，該個人資料獲得適當等級之保護，並應遵循下列事項：

(一) 本公司應注意傳輸接受國（地區）是否經中央目的事業主管機關限制個人資料跨國（境）傳輸，並應依據中央目的事業主管機關發布之限制規定辦理。

(二) 若個人資料揭露予國（境）外第三方或執行國（境）外個人資料委外作業，本公司應要求受託單位遵守個人資料保護法相關規定。

三十二、個人資料揭露予外部之第三方應遵循下列事項：

(一) 除依法得免告知之情形外，須依法令規定之方式或取得當事人書面同意後方可執行。

(二) 應確保僅揭露最少內容之個人資料項目。

(三) 與第三方進行個人資料傳遞時，應依本公司現有個人資料管理規範進行管控。

(四) 各種向第三方進行個人資料傳遞之紀錄，應予完整留存至少五年。

(五) 若以紙本郵寄投遞時，應依本公司相關文書處理規定以密件處理。

前項所稱第三方如為行政機關、司法機關等政府機關或其他相關機構者，必須有原始查詢文件（如：外部機構公函或查詢單等）。遇有案情特殊之緊急查詢，得由查詢機關首長或其書面指定人先以電話或公文傳真，經確認無誤後，依個案需求辦理。

除法令要求外，其他因業務需求需傳遞或複製個人資料予第三方時，應事先確認此第三方已與本公司簽訂載明雙方權利義務之契約或類似契約文件，作為執行依據。

三十三、個人資料委託外部單位蒐集、處理或利用時，應遵循下列事項：

(一) 應視情況於簽訂契約前對受託單位之現有安全控管措施進行了解與審查。

(二) 應確認契約內容符合相關法令要求。

(三) 應對受託單位進行至少包含下列事項之監督：

1. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
2. 確認受託單位依個人資料保護法採取適當之安全維護措施。
3. 確定受託單位可否進行複委託，如許可複委託，應要求受託人於複委託契約中約定複受託人應至少履行與受託人相同程度之個人資料保護義務。
4. 受託單位或其受僱人員違反個人資料保護法令或委託契約條款時，應通知本公司，並採行對應之補救措施。
5. 於必要時，可對受託單位於契約範圍內進行相關個人資料管理稽核作業。
6. 契約應載明若有可歸責於受託單位之責任，對當事人及本公

司之補償、損害賠償、和解或協商方式。

7. 對受託單位有保留指示者，其保留指示之事項。

8. 委託關係終止或解除時，應要求受託單位返還保存個人資料之載體，並刪除或銷毀儲存於受託人之個人資料。

(四) 委外契約內容若包括個人資料（如保密切結書等）時，契約書面資料之保存期間應與個人資料之保存期間一致。

(五) 受託單位若有處理大量或敏感個人資料時，應要求受託單位對其執行人員進行適當教育訓練。

(六) 應定期確認受託單位執行之狀況，並將確認結果記錄之。

第 七 章 人員管理

三十四、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適當控管措施。

三十五、本公司聘任或聘僱人員必須簽署接受並履行本公司人員委任契約或勞動契約（含保密相關協議）中所有有關個人資料保護的條款與條件，以及遵守所屬單位各項作業規章中所含個人資料保護規定與職責。

三十六、各單位主管於人員調離職時，須確認其保管之個人資料相關檔案與紀錄均已歸還，且其存取相關檔案與紀錄之權限皆已被取消；該調離職人員並應於相關表單中承諾於調離職後仍繼續遵守個人資料保護法令相關規定。

第 八 章 個人資料安全管理

三十七、本公司就個人資料之儲存與處理原則應考量其機密、風險及敏感性，並以合適之方式管理(包含但不限於資料傳輸、資料列印、資料銷毀及權限控管)。

三十八、各單位用於蒐集、處理與利用個人資料作業之電腦設備，其軟碟機、USB埠及燒錄式光碟機等，應採取適當控管措施。

三十九、資訊單位就備份資料應定期執行資料有效性測試，以確認備份資料之可讀性及儲存媒體之可用性。

四十、 本公司應於公開網站上以易於瞭解之形式，宣告「隱私權保護政策」，包含提供相關諮詢管道，且應明訂加入網站之相關使用者之權利。

四十一、本公司公開網站內容若涉及個人資料蒐集、處理及利用，應由業管單位會辦法令遵循單位後始可為之。

四十二、本公司各項關於個人資料存取權限之授予，應秉持業務與執行工作所需最小權限為原則。

四十三、就含有個人資料之系統，其系統存取權限管理者應定期請各單位主管確認存取人員權限之適切性。

四十四、資訊單位應依各單位之需求確保系統留存適當之個人資料存取紀錄，並採

用適當之防護機制。

四十五、本公司就所提供之電子商務服務系統，應採取下列資訊安全措施：

(一) 使用者身份確認及保護機制。

(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。

前項第六款、第七款所定措施，應定期演練及檢討改善。

第 九 章　認知、宣導及教育訓練

四十六、負責日常個人資料管理政策遵循之人員應能瞭解個人資料保護法令與實務，及具備具體落實之能力，並適時獲取與個人資訊管理有關的資訊。

所有人員應瞭解其本身在個人資料保護上的責任，並應依適當之程序保護及處理個人資料。

四十七、本公司應對所屬人員(含常駐於本公司並負責個人資料蒐集、處理或利用作業之委外人員) 進行個人資料保護之認知宣導與教育訓練。

前項認知宣導與教育訓練得採用會議、電子文宣、紙本文宣，或舉辦活動等各種方式進行。

第 十 章　設備安全管理

四十八、本公司應就存放或傳遞個人資料檔案之本公司主機電腦設備及其他媒介物，訂定相關管控措施並由權責單位管理。

四十九、各單位處理或儲存個人資料之設備，應依照本公司「資訊資產保護管理要點」、「個人電腦設備使用管理須知」，及「網路設備管理須知」等規範進行管控。

第 十一 章　個人資料使用紀錄、軌跡資料及證據之保存

五十、　各單位應在保存措施與所欲達成之個人資料保護目的間，具有適當比例之原則下，於必要範圍內，保存下列個人資料使用紀錄、軌跡資料及證據：

(一) 個人資料交付、傳輸之紀錄。

(二) 確認個人資料正確性及更正之紀錄。

(三) 提供當事人行使權利之紀錄。

(四) 個人資料刪除及銷毀之紀錄。

(五) 透過系統存取個人資料之紀錄。

(六) 備份及還原測試之紀錄。

(七) 所屬人員權限新增、變動及刪除之紀錄。

(八) 所屬人員違反權限行為之紀錄。

(九) 因應個人資料安全事故發生所採取行為之紀錄。
(十) 定期檢查含個人資料之資訊系統之紀錄。
(十一) 教育訓練之紀錄。
(十二) 相關稽核及改善程序執行之紀錄。

上述相關紀錄應至少保留五年。但法令或本公司另有規定者，從其規定。

五十一、個人資料之系統使用及紙本作業，應經適當授權並維持其內容之正確性。

五十二、核心小組成員應彙整所屬單位個人資料安全事故之完整證據，提交核心小組，由核心小組針對事故之原因進行檢討分析，並協調相關單位執行改善及預防措施，以避免事故重複發生，或預防潛在事故發生。

第 十二 章　個人資料安全稽核機制

五十三、本公司應將個人資料管理納入本公司內部控制及稽核制度，其相關查核程序、查核方式、執行頻率及程序依照本公司「稽核作業準則」規定辦理。

稽核單位應依據法令、本公司相關規章及外部標準訂定稽核項目，並據以實施查核。

五十四、本公司應將個人資料之保護納入法令遵循自行評量項目，並定期進行評量，以確保相關法令之遵循。

第 十三 章　個人資料安全維護之整體持續改善

五十五、各單位應依照本計畫及處理要點，執行並持續改善個人資料安全維護措施。

五十六、核心小組應依「個人資料管理風險自我評估報告」之結果，適時檢討修正本計畫及處理要點；如發現有違反法令之虞者，並應規劃改善及預防措施。

第 十四 章　附則

五十七、本計畫及處理要點如有未盡事宜，悉依有關法令及主管機關規定辦理。

五十八、本計畫及處理要點經總經理核定後，自發布日實施；修正時，亦同。