兆豐國際商業銀行個人資料檔案安全維護準則

103 年 2 月 7 日董事會核定施行
105 年 8 月 26 日董事會核定施行
105 年 9 月 29 日組織調整逕予修正
107 年 9 月 28 日董事會核定施行
108 年 2 月 22 日授權修正
111 年 3 月 4 日董事會核定施行

第一章　總則

第一條　(依據)

為加強本行個人資料檔案之管理、確保個人資料之安全，茲依據「金融監督管理委員會(以下簡稱「金管會」)指定非公務機關個人資料檔案安全維護辦法」及本行「個人資料保護管理政策」規定，訂定本準則。

第二條　(權責單位)

本準則由本行「個人資料保護管理政策」第三條所訂之個人資料統籌單位(以下簡稱「統籌單位」)，負責制定及維護。若修訂同時涉及總處、國內(外)分支機構之共同事項，依國內法規或國外法規變動而定，由各該統籌單位依職掌為之。

第三條　(個人資料保護機制)

各業務管理單位於職掌業務涉及個人資料之蒐集、處理或利用時，除遵循本準則外，應依職掌業務之特性，評估可能產生之個人資料風險，得視評估結果另行訂定職掌業務適用之個人資料保護機制、程序及措施；該個人資料保護機制、程序及措施與本準則內容牴觸者，本準則優先適用。

前項及其他依本準則訂定之個人資料保護機制、程序及措施，應先簽會統籌單位，如為作業規範之訂定，並應經　副總經理核定後施行，修正或廢止時亦同。

國外分支機構得依據機構所在地之個人資料保護規範，建立相關個人資料保護機制，並陳報海外業務處核定或備查。

第四條　(國外分支機構之管理措施)

國外分支機構應每季向海外業務處彙報個人資料保護之執行情形，並副知海外管理處。報告內容應包含但不限法令修訂情形、內外部檢查機關之查核問題及改善措施、個資事件發生及處理情況等。

海外業務處針對報告內容所列之缺失項目，應檢視國外分支機構之相關規範或作業流程是否須配合修正，必要時並應通知其他業務管理單

位。
第一項國外分支機構個人資料保護執行情形之報告時間及方式，由海外管理處訂定規劃。

第五條　(個人資料管理主管)
各單位應指定單位副主管乙名擔任個人資料管理主管，負責督導所屬單位執行本準則及相關個人資料保護機制、程序及措施，並指定甲級主管乙名擔任其代理人，惟未設置單位副主管之單位，個人資料管理主管及其代理人得均由甲級主管擔任。
個人資料管理主管及其代理人之聯絡資料應於個人資料管理主管通報系統建立，如有異動，應於接任人選到任後二個營業日內完成異動登錄。
各單位對於所保有之個人資料檔案現況，應依個人資料保護法(以下簡稱「個資法」)相關法令、本準則及各業務管理單位訂定之個人資料保護機制、程序及措施，每年至少查核確認乙次，並製作清冊後留存備查。

第六條　(個資事件因應機制)
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」)，統籌單位應訂定下列應變、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。
本行遇有重大個人資料事故者，應由統籌單位填具「金管會指定非公務機關個人資料檔案安全維護辦法」第六條附件「個人資料侵害事故通報與紀錄表」，於發現個資外洩後七十二小時內(例假日均納入時效計算)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。前項第三款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，將危及本行正常營運或大量當事人權益之情形。

第七條　(教育訓練)
人力資源處除對新進行員於進行時，辦理個資法相關訓練外，應每一年至少一次對行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、行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。

第八條（管理程序）

統籌單位應就下列事項，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個資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，並應確保符合個資法第六條第二項準用第七條第一項、第二項及第四項規定。

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，是否符合個資法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合個資法第七條之規定。

四、檢視一般個人資料之利用，是否符合個資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，並應確保符合個資法第七條之規定。

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，對受託人依個資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，檢視是否受金管會及其他主管機關限制並遵循之。

八、當事人行使個資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，並遵守個資法有關處理期限之規定。

(四)有個資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，應依個資法第十一條第一項、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，應依個資法第十一條第三項規定刪除、停止處理或利用。

前項第三款及第四款，有關個資法第七條當事人同意方式，除法規另有規定外，不以書面為限，惟仍應留存紀錄，以利事後舉證。

第九條（安全管理措施）

為維護所保有個人資料之安全，本行應採取下列資料及設備之安全管理措施：

一、訂定各類設備或儲存媒體或其他媒介物之使用及保管規範，包括但不限於實施適宜之存取管制、依媒介物之特性及其環境，建置適當之保護設備或技術，訂定妥善保管媒介物之方式，以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，應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。

個人資料以本行磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備為處理、利用者，由資訊處訂定前項之安全管理措施；個人資料以紙本或其他媒介物為處理、利用者，由統籌單位訂定前項之資料安全管理措施。

第十條（資訊安全措施）

對於本行電子商務服務系統，資訊處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，資訊處每年至少應辦理乙次演練及檢討改善並副知資訊安全處及統籌單位。

第十一條（權限限制）

各單位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，所屬人員並應約定保密義務。

第四章　個人資料之安全稽核、紀錄保存及持續改善機制

第十二條（查核項目）

本準則及相關個人資料保護機制、程序及措施之執行情形，應列入本行作業風險自我評估、內部控制制度自行查核、法令遵循自評及內部稽核項目。

第十三條（證據留存）

各單位執行本準則及相關個人資料保護機制、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備查。

各單位依個資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。

第十四條（自我評估報告）

各單位之個人資料管理主管，應檢視最近一年法令遵循自評、內部控制制度自行查核、內外部稽核報告及各單位另行發現之個人資料管理缺失及檢討措施，於每年一月底前向法令遵循處提出各單位個人資料管理之自我評估報告，並將該報告提供予單位內各業務辦理作業風險自評之主管，做為辦理與個資相關作業風險自評項目評估之參考依據。

法令遵循處應彙總各單位自我評估報告及另行發現之個人資料管理缺失及檢討措施，並於每年二月底前提出全行個人資料管理之自我評估報告。

前項之全行自我評估報告，授權總經理核定之。

針對第一、二項之自我評估報告中有違反法令之虞者，法令遵循處應自行或通知統籌單位及其他業務管理單位協調規劃、執行其改善及預防措施。

第十五條（檢討作業）

本準則由統籌單位每年至少檢討乙次；各業務管理單位訂定之個人資料保護機制、程序及措施，由各業務管理單位每年至少檢討乙次。

第十六條（未盡事宜）

本準則未盡事項，悉依相關法令、主管機關規定及本行相關規定辦理。

第十七條（核定層級）

本準則經董事會核定後施行，修正或廢止時亦同。