兆豐金融控股股份有限公司個人資料檔案安全維護準則

103 年 2 月 25 日第 5 屆第 22 次董事會訂定
104 年 9 月 22 日第 6 屆第 4 次董事會修正
105 年 8 月 23 日第 6 屆第 18 次董事會修正
109 年 10 月 27 日董事會授權逕行更正單位名稱，修正條文自 110 年 1 月 1 日生效
111 年 5 月 24 日第 8 屆第 12 次董事會修正

第一章　總則

第一條　（目的及依據）

為加強本公司個人資料檔案之管理，確保個人資料安全，特依「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」規定，訂定本準則。

第一條之一（權責單位）

本準則之權責單位為法令遵循部。

第二章　個人資料保護之規劃

第二條　（配置適當人力）

法令遵循部應依本公司業務規模及特性配置適當管理人員及資源，負責訂定及督導各單位執行本準則及相關個人資料管理機制、程序及措施。

前項個人資料管理機制、程序及措施授權總經理核定。

第三條（定期查核）

本公司各單位應依個人資料保護相關法令，每年辦理一次查核確認所保有之個人資料現況，界定其納入本準則所訂安全維護管理之範圍。

第四條　（風險評估）

本公司各單位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。
法令遵循部應依前項風險評估結果，訂定適當之個人資料管理機制。

第五條（個資事故因應機制）

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。

發生重大個人資料事故時，受通報單位應依「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」第六條附件格式，於發現個資外洩後七十二小時內(例假日均納入時效計算)通報金融監督管理委員會。但於其他法令另有規定時，並應依各該法令之規定辦理。依前項第三款研議之矯正預防措施，應委由公正、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。

第六條（教育訓練）

本公司應定期對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、員工之責任範圍及與本準則相關之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

第七條（管理程序）

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

四、檢視一般個人資料之利用，是否符合個人資料保護法第二十條規定蒐集之特定目的必要範圍。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,並應確保符合個人資料保護法第七條之規定。

五、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依個人資料保護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。

六、進行個人資料國際傳輸前，檢視是否受金融監督管理委員會限制並遵循之。

七、當事人行使個人資料保護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，並遵守個人資料保護法有關處理期限之規定。

(四)有個人資料保護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。

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

九、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，應依個人資料保護法第十一條第三項規定刪除、停止處理或利用。

第八條 （資料安全管理措施）

為維護所保有個人資料之安全，本公司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。

第九條（設備安全管理措施）

本公司就紙本、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保有之個人資料，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。

第十條 （人員管理措施）

為維護所保有個人資料之安全，本公司應採取下列人員管理措施：

一、各單位應檢視、確認各業務流程涉及蒐集、處理或利用個人資料之負責人員。

二、各單位應依執行業務之必要，設定相關人員接觸個人資料之權限，並控管其接觸情形。

三、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

第十一條（稽核機制）

為確保本準則及相關個人資料管理機制、程序及措施之落實，董事會稽核室應依本公司業務規模及特性，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；並應將相關機制列入內部控制及稽核項目。

第十二條（紀錄保存）

本公司各單位執行本準則所定各種個人資料保護機制、程序及措施，應記錄個人資料使用情況、留存軌跡資料或相關證據。

本公司各單位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，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。

第十三條（自我評估報告）

為持續改善個人資料安全維護，本公司保有個人資料之單位應每年至少提出一次相關自我評估報告，並辦理下列事項：

一、檢視、修訂本準則及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。

前項自我評估報告由法令遵循部彙總，陳報總經理核定。

第五章　附則

第十四條（未盡事宜）

本準則未盡事宜，悉依相關法令及本公司有關規定辦理。

第十五條（核定層級）

本準則經董事會通過後施行，修正或廢止時亦同。

「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」第六條附件格式

<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/單位:
_____</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小時通報金融監督管理委員會</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小時通報金融監督管理委員會，例假日均納入時效計算。