彰化銀行個人資料檔案安全維護計畫

中華民國 103 年 6 月 30 日第 23 屆第 29 次董事會制定
中華民國 105 年 12 月 23 日第 24 屆第 25 次董事會修正
中華民國 108 年 1 月 23 日第 25 屆第 20 次董事會修正
中華民國 111 年 1 月 24 日第 26 屆第 22 次董事會修正

第一條（制定宗旨及依據）

為落實個人資料檔案之安全維護與管理，本行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三條規定，訂定彰化銀行個人資料檔案安全維護計畫（以下稱本計畫）。

第二條（適用範圍）

本計畫適用於本行各項業務流程所蒐集、處理及利用之個人資料。

第三條（名詞定義）

本計畫名詞定義如下：

一、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。

二、媒介物：指保有之個人資料所存在之紙本、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之物體者。

三、重大個人資料安全事故：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。

四、軌跡資料：個人資料在蒐集、處理及利用過程中，所產生非屬於原蒐集個人資料本體之衍生資訊（包括但不限於軌跡檔案、當事人之帳號、存取時間、設備代號、網路位址）。

第四條（配置個人資料管理人員及資源）

本行各業務主管處應配置個人資料保護管理人員及相當資源，以規劃及執行本計畫。

第五條（界定個人資料之範圍）

本行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，界定其納入本計畫之範圍。

第六條（風險管理機制）

本行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。

第七條（個人資料蒐集、處理及利用）

本行對於個人資料之蒐集、處理及利用，應建立內部管理程序，內容包含下列事項：

一、蒐集、處理及利用之個人資料包含個人資料保護法（以下稱個資法）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、第二項及第四項之規定。

二、個人資料之蒐集，除個資法有特別規定者外，應履行告知義務，並確認告知之內容及方式是否合法妥適。

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，並確保符合個資法第七條之規定。

四、確認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，應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時，應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，檢視是否係受金融監督管理委員會

限制之範圍。

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。

第八條（個人資料安全管理措施）

為維護所保有個人資料之安全，本行應就下列事項訂定個人資料安全管理措施：

一、電子商務服務系統之資訊安全措施：

（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。

（八）定期對前二目所定措施進行演練及檢討改善。

二、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。

三、有加密需要之個人資料，於蒐集、處理或利用時，採取適當之加密措施。

四、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。

五、對保有之個人資料存在於媒介物者應採取之設備安全管理措施：

(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。

六、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。

第九條（緊急應變、通報及預防機制）

為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，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。

遇有重大個人資料安全事故者，應於七十二小時內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。

第十條（教育訓練）

本行應定期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、責任範圍與各種個人資料保護機制、程序及措施。

第十一條（個人資料安全稽核機制）

依本計畫所訂個人資料保護機制、程序及措施，應納入內部稽核及內部自行查核範圍。

第十二條（留存紀錄）

本行執行依本計畫所訂個人資料保護機制、程序及措施，應記錄其個人資料使用情況，並留存軌跡資料或相關證據。

第十三條（特定目的消失或期限屆滿）

個人資料蒐集之特定目的消失或期限屆滿時，除法令另有規定外，應刪除、停止處理或利用所保有之個人資料，並留存下列紀錄：

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。

前條及前項之軌跡資料、相關證據及紀錄，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）

為持續改善本行之個人資料安全維護作業，相關業務主管處應每年定期就其執行情形，提出自我評估報告。

前項自我評估報告經彙總後，陳請總經理核定，並提報常務董事會備查。

自我評估報告應就有違反法令之虞之個人資料保護事項，進行規劃、執行改善及採取預防措施。

第十五條（授權事項）

依本計畫所訂個人資料保護機制、程序及措施，授權總經理核定之，相關業務主管處應定期檢視及為必要之修訂。

總行因遵循海外單位所在地之個人資料保護法規，需另訂相關機制、程序及措施時，得比照前項規定辦理。

第十六條（施行與修正）

本計畫提請董事會決議通過後實施，修正時亦同。