富邦金控

富邦金融控股股份有限公司暨子公司
個人資料檔案安全維護及
業務終止後個人資料處理辦法

文件編號：FHC-O-PDP-3-20230413
核准日期：2023/04/13
生效日期：2023/04/14
主辦單位：風險控管處作業風險暨綜合規劃部
版　　序：第 11 版

富邦金控

目錄

富邦金控

第一章　總則

第一條　訂立目的

為落實富邦金融控股股份有限公司（下稱「本公司」）及本公司營業執照所載之子公司（下稱「子公司」）個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失、洩漏或濫用，及規範業務終止後個人資料處理方法，依照「富邦金融控股股份有限公司暨子公司個人資料保護管理政策」，特制定「富邦金融控股股份有限公司暨子公司個人資料檔案安全維護及業務終止後個人資料處理辦法」（下稱「本辦法」），俾利遵循。

第二條　適用範圍

本辦法適用於本公司及子公司，海外子公司依其當地政府或地區相關法令另有規定者，從其規定。

子公司除主管機關另有規範而須另行制定「個人資料檔案安全維護及業務終止後個人資料處理辦法」外，得沿用本辦法或另行訂定。若沿用本辦法為其「個人資料檔案安全維護及業務終止後個人資料處理辦法」，應依子公司分層負責核定。

子公司應依本辦法原則督導其轄下子公司。

第二章　配置管理之人員及相當資源

第三條　個人資料保護督導委員會之設立

本公司在風險管理委員會下設立「個人資料保護督導委員會」，督導個人資料保護相關事宜。個資保護監督單位由風險控管處作業風險暨綜合規劃部擔任，協助建置個人資料保護體系、制度及相關教育訓練。

第四條　個人資料保護管理目標之實現

各單位主管為單位內個資保護管理工作負責人，除負責個資保護管理政策及相關辦法之遵循，應指派人員擔任個資保護管理相關工作，確保本公司個人資料保護管理目標之實現；各單位應遵循下列要求：

一、符合個人資料保護之各項法令規定、客戶契約及其他相關規範要求。

二、維護個人資料當事人之人格權，提供其個人資料的合法自主權

三、對個人資料之蒐集、處理及利用過程，將以誠實及信用方法為之，不逾越特定目的之必要範圍、並應與蒐集之目的具有正當合理之關聯；

四、提供個人資料檔案適當之安全措施，以確保本公司得以盡善良管理之注意義務；

五、確保內外部規範落實程度，並訂定個人資料保護之可接受的風險程度與因應措施；

六、對個人資料委外第三方之管理，確保第三方對於個人資料善盡保護責任。

第五條　個資保護管理組織架構及職責

個資保護管理組織架構及職責另行訂定之。

第三章　界定個人資料範圍

第六條　個人資料檔案

企業資訊流概覽圖(Business Information Framework，以下簡稱「BIF」)：以業務為導向，分析個人資料檔案資訊流及管理現況而呈現之個人資料流概況。

個人資料檔案清冊：依個人資料檔案資訊流及管理現況而建立之清冊。

個人資料檔案群組：

群組	群組說明
高風險個人資料	含特種個人資料： 含病歷、醫療、基因、性生活、健康檢查或犯罪前科之個人資料檔案者。
	含性質較為特殊、具敏感性或易被利用造成內外部客戶損失之資料。 如：含信用卡卡號、身分證字號、護照號碼、銀行存款帳號、其他財務資訊或未成年人及弱勢成人之個人資料檔案。 上述未成年人定義為未滿 20 歲之人；弱勢成人定義為受輔助宣告及受監護宣告之人。
一般直接識別個人資料	除高風險個人資料以外，其檔案內含有可識別特定個人者。 如：姓名、網路會員帳號。
間接識別個人資料	僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。

	如：出生年月日、特徵、婚姻、家庭、教育、職業、社會活動、聯絡方式、可辨別國籍等。

第七條　個人資料檔案清查

公司各單位須清查個人資料檔案，識別其流向，並建立 BIF 及「個人資料檔案清冊」，如清查結果無個人資料檔案，則無建立 BIF 及「個人資料檔案清冊」之必要。

考量資訊單位涉及之個人資料皆存放於系統，經清查個人資料檔案後，僅須建立「個人資料檔案清冊」。

第八條　個人資料檔案清冊更新

擁有個人資料檔案之單位(即個人資料管理單位)應至少每年檢視流程盤點並更新 BIF（資訊單位除外）及「個人資料檔案清冊」。

首次清查結果無個人資料檔案之單位及擁有個人資料檔案之單位，當個人資料檔案有重大異動或推出新種產品或服務時，權責單位應執行流程盤點及個人資料檔案清查，依盤點及清查結果增修 BIF 及「個人資料檔案清冊」，並經單位主管簽核。

第四章　個人資料之風險評估

第九條　個人資料管理衝擊分析

個人資料管理衝擊分析：分析目前個人資料檔案控管措施與個人資料保護之各項法令規定之差異。

第十條　個人資料管理衝擊分析之執行時機

擁有個人資料檔案之單位首次完成個人資料檔案盤點、BIF、個人資料檔案清冊後，須執行個人資料管理衝擊分析，之後每年定期執行。

第十一條　個人資料保護自我評估

個人資料管理單位，依據「富邦金融控股股份有限公司暨子公司個人資料保護自我評估管理辦法」對持有的個人資料所存在之風險進行自我評估，並定期提出相關自我評估報告及陳報作業風險暨綜合規劃部。

第十二條　個人資料保護管理資訊呈報

應定期檢視本公司面臨之個人資料內、外部議題影響與關注方對於個人資料保護之期望，以期及早因應相關風險、採取行動。並將潛在重要事項彙整於個人資料保護督導委員會進行呈報。

若涉及個人資料檔案之業務、產品、流程、系統有重大變更時，權責單位應依照內部規範進行風險評估，於上線前將個人資料隱私保護納入設計考量。

應針對個人資料管理目標制定有效性量測指標及量測週期，確保目標達成之落實程度，並針對未達標之事項進行改善作業。

第五章　使用紀錄、軌跡資料及證據保存

第十三條　個人資料使用紀錄之保存

個人資料管理單位應製作文件記錄個人資料使用情況、留存自動化機器設備之軌跡資料或相關證據保存，以落實相關個人資料保護管理。本公司執行本辦法所定各種個人資料保護機制、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。相關軌跡資料、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　個人資料侵害事故證據之保存

當個人資料侵害事故發生時，應執行調查活動，以辨識肇事原因與區分人員責任，為能在紛爭處理與訴訟程序中提供完整的證據。應訂定個人資料鑑識規範，包含證據封存與保存、證據復原與重建、證據分析與鑑識等。

第六章　個人資料安全維護之整體持續改善

第十五條　個人資料保護管理體系之運作架構

個人資料保護管理體系運作之架構以「計畫-執行-檢查-行動」為基礎，在日常管理與營運上，落實資訊安全及個人資料保護法相關的規定。

第十六條　個人資料保護管理體系之持續改善

依據前條檢查及量測的結果及建議，執行矯正與預防措施，若屬內、外部稽核或重要個人資料事故，應包含根因鑑別程序，以持續改善個人資料保護管理體系。

第七章　定義及說明

第十七條　蒐集

指以任何方式取得個人資料。

第十八條　處理

指為建立或利用個人資料所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

第十九條　利用

指將蒐集之個人資料為處理以外之使用。

第八章　個人資料蒐集

第二十條　個人資料蒐集之特定目的

個人資料之蒐集，除本辦法第二十六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，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之個人資料。

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。

第四款所稱同意，指當事人經蒐集者告知個人資料保護法所定應告知事項後，所為允許之意思表示。

公司明確告知當事人本辦法第二十二條各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依上該第四款之規定表示同意。

蒐集者就個人資料保護法所稱經當事人同意之事實，應負舉證責任。

蒐集者知悉或經當事人通知依第一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。

第二十一條　個人資料蒐集特定目的之定期檢視

向當事人蒐集個人資料時，應檢視其特定目的及是否符合相關法令之要件，每年應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，並留存確認軌跡，呈主管核閱。

第二十二條　個人資料蒐集之告知

向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公司的名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依個人資料保護法第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

第二十三條　個人資料蒐集之免為告知

向當事人蒐集個人資料時，經檢視有下列情形之一者，得免為前條之告知：

一、依法律規定得免告知。

二、個人資料之蒐集係公司履行法定義務所必要。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第二十四條　個人資料蒐集之告知方式

向當事人蒐集個人資料之告知方式，得於契約、申請書、通知書、委託書等載明相關告知事項，告知內容應經法務或法令遵循單位審閱並經分層負責核定，以確認其妥適性。

第二十五條　未成年人或弱勢成人個人資料蒐集之告知

依照個人資料保護相關法令規範之告知方式執行法定告知，若當事人為未成年人或弱勢成人，另須取得當事人之法定代理人或監護人同意，並應保存告知紀錄。

第二十六條　特種個人資料之蒐集

蒐集個人資料時，應檢視所蒐集之資料是否含有特種個人資料。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，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公司履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、為協助公務機關執行法定職務或公司履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

五、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用個人資料保護法第八條及第九條規定；其中前項第五款之書面同意，準用個人資料保護法第七條第一項、第二項及第四項規定，並以書面為之。

第九章　個人資料處理與利用

第二十七條　個人資料間接蒐集之告知

公司依個人資料保護法第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人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。

有下列情形之一者，得免為前項之告知：

一、有本辦法第二十三條所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集 者依其揭露方式，無從識別特定當事人者為限。

第一項之告知，得於首次對當事人為利用時併同為之。

第二十八條　個人資料處理之特定目的

個人資料之處理，除本辦法第二十六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，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之個人資料。

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。

第四款所稱同意，指當事人經蒐集者告知個人資料保護法所定應告知事項後，所為允許之意思表示。

公司明確告知當事人本辦法第二十二條各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依上該第四款之規定表示同意。

對個人資料處理，應檢視其特定目的及是否符合相關法令之要件。蒐集或處理者知悉或經當事人通知依第一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。

第二十九條　個人資料處理或利用之原則

個人資料之處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第三十條　個人資料處理或利用之安全維護措施

個人資料之處理或利用，應有適當安全維護措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施。

第三十一條　個人資料檔案提供予第三方

如須提供個人資料檔案予第三方(例如：主管機關、會計師、檢警調機關、稅務機關、法院等)，應予紀錄，並經主管簽核。

第三十二條　利用個人資料行銷

子公司利用個人資料行銷，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，並通知所屬單位人員。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。

第三十三條　個人資料利用之特定目的

對個人資料之利用，除本辦法第二十六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，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、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、經當事人同意。

六、有利於當事人權益。

第五款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

對個人資料利用，應檢視其特定目的及是否符合相關法令之要件。

第三十四條　特定目的外個人資料之利用

特定目的外個人資料之利用，應事先取得主管書面同意。

經主管書面同意後，若須取得當事人之書面同意時，應明確告知當事人特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，請當事人簽署同意書。

應將特定目的外利用之個人資料更新於個人資料檔案清冊。

第三十五條　特種個人資料之處理或利用

病歷、醫療、基因、性生活、健康檢查及犯罪前科之特種個人資料屬高度機敏性，處理或利用特種個人資料應有事前或事後之適當安全維護措施。

第三十六條　個人資料之國際傳輸

個人資料國際傳輸不得涉及國家重大利益或以迂迴方法向第三國（地區）傳輸個人資料規避個人資料保護法或違反國際條約或協定有特別規定；若接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞，不得進行國際傳輸；進行個人資料國際傳輸前，應檢視是否受金管會限制並遵循之。

第三十七條　個人資料蒐集之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，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），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。

第三十八條　違反蒐集、處理或利用個人資料之處理

違反蒐集、處理或利用個人資料規定者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

第十章　個人資料委外蒐集、處理與利用

第三十九條　委託蒐集、處理及利用個人資料

受委託蒐集、處理及利用個人資料者(下稱受託者)，於個人資料保護法之適用範圍，視同委託機關。委託單位應妥善監督受託者，該監督至少應包含下列事項：

一、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。

二、受託者僅得於委託單位指示之範圍內，蒐集、處理或利用個人資料。如受託者認為委託單位之指示有違反個人資料保護法、其他個人資料保護法律，或其法規命令者，應立即通知委託單位。

三、受託者為防止個人資料被竊取、竄改、毀損、滅失或洩漏所採取技術上及組織上之必要措施，其標準不得低於個人資料保護法及其施行細則之規定。

四、受託者或其受僱人違反個人資料保護法、其他個人資料保護法律，或其法規命令時，應立即通知委託單位及採行補救措施。

五、委託關係終止或解除時，受託者應返還個人資料載體，及刪除、銷毀受託者履行委託契約以儲存方式而持有之個人資料，並出具切結書或相關證明。

倘受託者或其受僱人或再受託者違反上開監督事項，致公司受有損害或損失時，受託者應賠償或補償公司，其範圍包括但不限於受第三人求償時所支出之律師費及商譽損失。

第四十條　委外蒐集、處理及利用個人資料之契約

除主管機關「金融機構作業委託他人處理內部作業制度及程序辦法」規範委外契約應載明事項外，前條相關監督事項及受託者的責任亦應規範於委外契約，要求受託者遵守。

第四十一條　對受託者之監督

委託他人蒐集、處理或利用個人資料時，委託單位應對受託者為適當之監督，有複委託者，其監督及於約定之受託者。

第四十二條　對受託者執行個人資料保護狀況之確認

委託單位應定期確認受託者執行個人資料保護措施之狀況，並應將確認結果予以記錄，呈主管核閱。

第十一章 個人資料當事人及其權利

第四十三條　當事人權利

當事人權利：指當事人就其個人資料依個人資料保護法規定得行使之權利，包含個人資料之查詢、請求閱覽，及請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及刪除。上該權利不得預先拋棄或以特約限制之。

第四十四條　當事人

當事人：指個人資料之本人。

第十二章 當事人權利行使之受理

第四十五條　當事人權利行使之受理窗口

擁有個人資料檔案且直接與客戶有業務往來之單位應設置當事人權利行使之受理窗口。

第四十六條　當事人權利行使之受理記錄

受理當事人權利之行使，應予記錄。

第四十七條　受理當事人權利行使之身分確認

受理當事人權利之行使，應確認當事人之身分，如有不符，應拒絕受理，並應提供當事人行使權利之方式，及告知所需支付之費用，與應釋明之事項。

前項當事人如為未成年人或弱勢成人時，除應確認當事人身分外，亦應確認當事人之法定代理人或監護人身分，並應取得當事人之法定代理人或監護人同意，以保障當事人之隱私與權益。

第四十八條　當事人申請資料之確認

為確保申請的正確性與合理性，應確認申請之個人資料項目與公司持有之資料相符。

第四十九條　當事人權利行使之准駁

若有下列情形之一者，得拒絕查詢、閱覽或製給複製本之申請：

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

二、妨害公務機關執行法定職務。

三、妨害公司或第三人之重大利益。

若有下列情形之一者，得拒絕當事人申請刪除、停止處理與利用個人資料：

一、有法令規定。

二、未達契約約定之保存期限。

三、有理由足認刪除將侵害當事人值得保護之利益。

四、其他不能刪除之正當事由。

當事人請求查詢、閱覽或製給複製本時，應於十五日內為准駁之決定；必要時得予延長，惟延長期間不得逾十五日，並應將其原因以書面方式通知當事人。

當事人請求補充、更正、刪除及停止蒐集、處理或利用時，應於三十日內為准駁之決定;必要時得予延長,惟延長期間不得逾三十日，並應將其原因以書面方式通知當事人。

第五十條　受理當事人行使查詢、閱覽或請求製給複製本

公司應依業務特性制定當事人行使查詢、閱覽或請求製給複製本之申請書，或將當事人請求之內容納入既有之申請書，前開申請書經法務或法令遵循單位審閱及分層負責核定後供當事人行使權利。

當事人行使其個人資料查詢、閱覽或請求製給複製本涉及不同單位時，當事人應填寫申請書，經受理窗口辨識當事人身分無誤後，將申請書交付相關權責單位處理。

當事人查詢、閱覽或請求製給複製本，得酌收必要成本費用。

第五十一條　受理當事人行使補充、更正權利或要求刪除、停止蒐集、處理與利用個人資料

應維護個人資料的正確性，並應主動或依當事人之請求更正或補充。

當事人至營業場所申請補充或更正其個人資料，應填寫申請書，並經主管核准。

當事人申請刪除、停止蒐集、處理與利用其個人資料，應填寫申請書，並經主管核准。

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

第十三章 當事人權利行使之處理及回覆

第五十二條　個人資料複製本之提供

提供當事人個人資料之複製本須與公司內部資料一致，經主管覆核，於確認身分無誤後，以加密或文件密封方式提供當事人，並留存副本或其他足以顯示原貌之佐證資料，及當事人簽收紀錄或以其他足以確認送達當事人之方式為之。

第五十三條　個人資料之更正或補充

因可歸責於公司之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第五十四條　個人資料之停止蒐集、處理、利用或刪除

應當事人請求於停止蒐集、處理、利用或刪除個人資料時，權責單位應檢視「個人資料檔案清冊」，並確認當事人訴求內容及當事人與公司往來之業務，經主管核准後，始得停止蒐集、處理、利用或刪除個人資料，並留存稽核軌跡及通知當事人之記錄。

第五十五條　當事人權利行使處理及回覆情形之追蹤

受理窗口應定期追蹤當事人權利行使之處理及回覆情形，並呈主管核閱。

第五十六條　當事人爭議之申訴

公司於拒絕當事人請求或發生爭議時，應提供當事人提出申訴之管道及聯繫方式，並做成紀錄(其中包含拒絕理由及通知當事人之方式)。

第十四章 人員管理

第五十七條　個人資料保護安全管理措施

公司應依據業務性質、業務流程、個人資料存取環境、個人資料之範圍及個人資料傳輸工具與方法等因素，採取安全管理措施。

第五十八條　人員管理措施

公司應採取下列人員管理措施：

一、依據職能分工、權責劃分、授權管理及作業之必要，設定所屬人員不同之權限並控管之，且定期確認權限內容設定之適當與必要性，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。

二、所屬人員應負保密義務。

三、晉用人員時,應由其填具保密切結書;離職時應取消其識別碼，並收繳其通行證、卡及相關公司證件。

四、各單位應指派人員負責個人資料檔案與帳號權限之管理。人員職務異動時，應辦理移交，並調整其權限。

五、應設定螢幕保護程式啟動時間，離開座位前，應登出電腦或鎖定螢幕。

六、下班前，應將電腦關閉或登出，筆記型電腦應予上鎖或存放於上鎖櫃中。

七、離開會議室前,應擦拭白板上的文字,並將會議書面資料帶走。

第十五章 作業管理

第五十九條　個人資料檔案作業管理措施

公司對個人資料檔案應採取本章各條所列之作業管理措施。

第六十條　個人資料傳輸之控管

傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密或保護機制，並確認資料收受者之正確性。

一、實體紙本個人資料檔案之傳輸

(一)含高風險個人資料及一般直接識別個人之個人資料檔案，無論進行公司內部傳輸或公司以外傳送，應適當彌封，並考量加入浮水印或以其他適當管控方式進行保護。

(二)針對特種個資之個人資料檔案，並應採用確認送達對方之傳遞方式。

二、電子個人資料檔案之傳輸

(一)個人資料檔案若存放於磁帶、光碟、可攜式或外接式儲存媒體中，應加密或以其他適當管控方式進行保護，並由專人傳遞、建立簽收機制。

(二)含高風險個人資料或一般直接識別個人之個人資料檔案，無論內部傳輸或對外傳送，應將重要資料加密或以其他適當管控方式(如專線或以壓縮檔設定密碼等)進行保護。

第六十一條　個人資料檔案保存之管理措施

個人資料檔案之保存應採取下列管理措施：

一、實體紙本個人資料檔案之保存

(一)對於非以電腦處理之個人資料檔案，應責成專人或專責單位管理，建立檔案分類整理、更新及借閱等機制。

(二)應建立實體紙本控管機制，確保個資檔案之妥善保存及其完整性，若需封箱保存時，應適當使用標示機制，標示不宜洩露過多資訊。實體紙本保管環境應注意防潮及防火，以確保實體紙本資料之安全、可用性。

(三)含高風險個人資料及一般直接識別個人之個人資料檔案，應隨時妥善收存於上鎖櫃中或受管制之場所。

(四)於下班前，應將實體紙本個人資料檔案存放於上鎖櫃中或受管制之場所。

(五)應訂定個人資料檔案保存年限；若有法令規定者，保存期限不得低於法令要求；且非有特殊理由，原則上不得將個人資料檔案之保存期限定為永久保存。

(六)針對列印、影印、傳真或掃描等輸出設備，應建立密碼或其他適當管控方式。列印、影印或傳真收發含高風險個人資料及一般直接識別個人之個人資料檔案應立即領取，並取走原始文件，以避免個人資料外洩。無人領取的文件應由專人定時收取並妥善保管，設簿登記，並經主管核閱，超過三天以上仍無人領取，立即銷毀。

(七)針對個人資料存在於紙本文件，應建立適宜之存取管制。

二、電子個人資料檔案之保存(包含磁碟、磁帶、光碟片、電話晶片、電腦、主機設備或其他媒介物)

(一)對於以電腦處理之個人資料檔案，應責成專人或專責單位管理，建立備援制度，並應於該檔案之建檔、使用、更新、更正或刪除時，建立存取控制之管理機制。

(二)針對所保有之個人資料內容，應採取適當之保護管控(如：加密、設定開啟密碼等)。

(三)對於個人資料之備份資料，應採取適當之保護管控(如:加密、存取管控等)；備份資料之儲存媒體亦應以適當方式保管，且定期進行備份資料之抽樣測試，以確保備份之有效性。

(四)應訂定各類檔案保存年限；若有法令規定者，保存期限不得低於法令要求；且非有特殊理由，原則上臨時性之個人資料檔案存放於個人電腦，使用完畢應立即刪除。

(五)除有業務需求並經主管核准，個人資料檔案不應存放於公用資料夾或公用電腦。

(六)資訊單位應針對個人電腦使用制訂相關控管保護機制。

(七)資訊單位應針對科技環境進行監控，並針對特定之外部攻擊進行防禦及處理。

(八)資訊單位應視資料及系統之安全性，採行必要之保護、監控與記錄保存等措施，偵測及防制電腦病毒、其他惡意軟體或行為，以防範電腦系統被侵入、破壞、竄改、刪除。

第六十二條　個人資料檔案銷毀之管理措施

個人資料檔案之銷毀應採取下列管理措施：

一、個人資料檔案銷毀須經主管事前核准，由兩人(含)以上會同辦理，並紀錄銷毀日期、內容、數量、銷毀方式、執行銷毀人員等，呈主管核閱。

二、儲存個人資料之媒體或資訊設備於廢棄或移轉與他人前，應依前款規範確實刪除媒體中所儲存之資料，或以物理方式破壞之，如另有備份檔亦應刪除。

三、當事人要求刪除個人資料檔案時，若依法令規定或契約約定之保存期限、有理由足認刪除將侵害當事人值得保護之利益或其他不能刪除之正當事由等情形，應以停止處理及利用代替刪除。

第十六章資訊設備管理

第六十三條　利用資訊設備蒐集、處理或利用個人資料之管理措施

利用資訊設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：

一、於資訊設備上設定認證機制，對有存取個人資料權限之人員進行識別與控管。人員異動時應及時更新其使用權限。

二、認證機制使用帳號及密碼之方式時，應使用優質密碼並定期更換密碼。

三、應拒絕未授權之存取行為，並設定警示與相關反應機制，針對未授權存取行為應保留稽核軌跡，且加強事後稽查追蹤。

四、對於存取個人資料之終端機進行帳號及密碼認證，以識別並控管之。

五、個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且人員不得共用身分識別帳號及密碼。

六、主管應事先核定使用者存取個人資料應用程式之權限。

七、各單位應定期檢核其帳號及權限之合理性，並留存軌跡及呈主管核閱。

八、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

九、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

十、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。

十一、 個人電腦不得安裝檔案分享軟體。

十二、 於測試環境不得使用真實個人資料，如有使用真實個人資料之情形時，其資料應進行遮蔽或變造。

十三、 處理個人資料之資訊系統如有變更時，應確認其安全性並未降低。

十四、 應制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。

十五、 運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。

十六、 妥善保存認證機制及加密機制中所運用之密碼，並應建立密碼交付程序。

十七、 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，應採取適當之加密措施。

十八、 針對複製、備份之個人資料檔案，應有適當之保護措施。

第六十四條　電子商務服務系統之資訊安全措施

提供電子商務服務系統，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。

第一項第二款所定之「個人資料顯示之隱碼機制」，係指在不影響正常交易資訊顯示情形下，隱碼達去識別化效果。如電子商務服務系統已對客戶身分為有效辨識，為確認交易必要資訊、確保交易正確性及取得佐證資料等目的，系統所顯示之轉出(入)帳號、交易金額、帳戶餘額及註記等資料，得不採行上開隱碼機制。惟為維護客戶個人資料安全，電子商務服務系統於交易過程顯示或列印之個人資料，仍應在不影響前述目的下，儘量以去識別化之隱碼方式處理。

第一項第六款、第七款所定措施，應定期演練及檢討改善。

第十七章 實體環境安全

第六十五條　個人資料實體檔案儲存之防護

對存有個人資料實體檔案儲存之處所，或儲存之主機、週邊設備及相關設施，應加強天然災害及其他意外事故之防護，並建立危機處理應變及通報機制。

第六十六條　個人資料檔案實體安全之維護

為維護個人資料檔案實體安全，公司所屬人員應遵循「富邦金融控股股份有限公司暨子公司門禁安全管理辦法」。

第六十七條　個人資料檔案儲存場所之控管

設有置放個人資料檔案與有儲存個人資料檔案之電腦設備之專門場所者，應建立門禁控管及實體安全維護措施(如監視設備、窗戶開啟感應等)。

第六十八條　辦公場所之控管

進出門禁時，應提高警覺以防止可疑人士尾隨進入辦公場所，並隨時注意辦公環境內是否有可疑人士。

第六十九條　檔案室或倉庫之門禁管理

辦公室內檔案室或倉庫，實施必要之門禁管理。

第七十條　作業環境之防災設備

針對不同作業環境，建置必要之防災設備。

第十八章 個人資料事故之預防

第七十一條　個人資料事故預防

在日常管理與營運上，以「計畫-執行-檢查-行動」為基礎，落實資訊安全及個人資料保護法相關的規定，以預防個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故(以下簡稱事故)。

第七十二條　個人資料檔案衝擊分析

透過個人資料檔案衝擊分析，辨識潛伏不合規之風險，建立改善措施以預防個人資料事故。

第十九章 個人資料事故之通報

第七十三條　重要及一般個人資料事故

事故發生單位應就下列指標判斷為一般或重要個人資料事故：

一、重要個人資料事故：符合下列要項之一，即屬重要個人資料事故。

(一)事故發生單位評估，該事故將造成公司名譽重大損害或影響健全經營之虞；

(二)接獲中央目的事業主管機關，司法機關或相關政府機關通知;

(三)接獲消費者保護組織之通知 ；

(四)接獲媒體之通知或已於媒體揭露；

(五)因同一原因事實造成十位(含)以上當事人權利受侵害之虞；

(六)因同一原因事實造成當事人提出侵害賠償金額並經公司評估達重要作業風險事件預估損失金額門檻。

二、一般個人資料事故

非重要個人資料事故視同一般個人資料事故。

第七十四條　個人資料事故之通報

事故發生單位經判斷有發生個人資料事故之可能性，應依「富邦金融控股股份有限公司暨子公司作業風險呈報及管理辦法」或公司相關規範進行通報。

第七十五條　重大個人資料事故之通報

事故發生單位發生金管會所規範之重大個人資料事故時：

一、事故發生單位應依重要作業風險事件通報規範及「富邦金融控股股份有限公司暨子公司重大事件通報主管機關作業準則」辦理通報，並應於發現個資外洩當日立即填報「個人資料侵害事故通報表」(詳如附件一)通報風控處作業風險暨綜合規劃部。

二、風控處作業風險暨綜合規劃部於完成審視呈核後儘速轉送稽核處，由稽核處於發現個資外洩後七十二小時內填報「個人資料侵害事故通報與紀錄表」(詳如附件二)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；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，將危及公司正常營運或大量當事人權益之情形。

第二十章 一般個人資料事故之應變機制

第七十六條　個人資料事故之調查及通知

事故發生單位應調查事故真實性、遭竊、外洩等資料的數量及範圍，並進行數位證據及紙本證據蒐證以利法律舉證，經確認為個人資料事故時，應於內部簽核後依照個人資料保護相關法令規範之告知方式執行法定告知，並應保存告知紀錄，通知當事人之內容應包括個人資料被侵害之事實及已採取之因應措施及諮詢服務專線，使當事人瞭解相關狀況，並提供後續查詢及協助。

第七十七條　個人資料事故之應變及改善措施

如可歸責於公司之事由而造成個人資料事故，應採取應變措施其中包括控制當事人損害之方式，以降低或控制損害之範圍，並建立改善措施，以防止事故再次發生。

第二十一章 本公司所規範之重要個人資料事故或金管會所規範之重大個人資料事故之應變機制(以下分別簡稱重要個人資料事故及重大個人資料事故)

第七十八條　個資緊急事故應變小組

為因應重要或重大個人資料事故之處理，應成立個資緊急事故應變小組，成員包含個資緊急事故應變小組召集人、事故發生、事故管理、資訊、公關媒體、稽核及法務或法令遵循單位等功能單位。事故發生單位經判斷為重要或重大個人資料事故，應通知事故管理單位及個資緊急事故應變小組召集人。

第七十九條　個資緊急事故應變小組會議之召集

個資緊急事故應變小組召集人接獲重要或重大個人資料事故時，視個人資料事故之影響程度與嚴重性，得召開個資緊急事故應變小組會議，領導緊急應變、掌握事故之資訊並進行決策；於重要或重大個人資料事故處理完成後，召開事故檢討會議，研議矯正及預防措施，以矯正及預防類此事故。

第八十條　個人資料事故之處理

事故發生單位應調查事故真實性、遭竊、外洩等資料的數量及範圍，並進行數位證據及紙本證據蒐證以利法律舉證，經確認為個人資料事故時，除應控制當事人損害外，於內部簽核後，依照個人資料保護相關法令規範之告知方式執行法定告知，並應保存告知紀錄，通知當事人之內容應包括個人資料被侵害之事實及已採取之因應措施及諮詢服務專線，使當事人瞭解相關狀況，並提供後續查詢及協助。

第八十一條　事故管理單位之責任

事故管理單位接獲重要或重大個人資料事故通報後，應立即通知個資緊急事故應變小組召集人、協助召集人召開會議，並協調、追蹤改善措施。

第八十二條　數位證據之蒐證

如個人資料事故與資訊系統有關，資訊單位需協助事故發生單位進行數位證據蒐證以利法律舉證，並調查根因及檢討改善。

第八十三條　媒體危機之處理

公關單位應監控媒體報導，視需要並依照「富邦金融控股股份有限公司暨子公司媒體危機處理準則」對外發佈書面聲明稿、對內部員工溝通，並由客服單位協助與消費者保護機構溝通及對客戶 Q&A。

第八十四條　對主管機關之通報

如符合「富邦金融控股股份有限公司暨子公司重大事件通報主管機關作業準則」之通報標準或重大個人資料事故，應依該要點規定通報中央目的事業主管機關。

第八十五條　法務或法遵單位之責任

法務或法令遵循單位應協助相關單位瞭解事故是否有違反個人資料保護相關法令，並視需要提供法律諮詢服務。

第二十二章　業務終止後個人資料處理程序

第八十六條　業務終止後個人資料處理程序之適用

本程序適用於個人資料保護管理體系內之業務及其業務相關部門，於業務終止後應如何適切處理該業務個人資料檔案。

第八十七條　業務終止

業務終止係指公司使一部或全部業務相關之當事人與公司繼續之契約關係向將來消滅的意思表示，可能包含下列情況：公司存續部分業務終止、公司購併行為、公司清算及解散等。

第二十三章　業務終止後個人資料檔案管理

第八十八條　對業務移轉應遵循之程序

一部或全部業務移轉他公司，應遵循以下程序。

一、應盤點該終止業務之相關個人資料檔案，並造冊管理。

二、依據個人資料檔案清冊，辦理個人資料檔案移交手續。移交手續應由業務單位辦理，移交人、接交人及監交人須同時在場點交。個人資料檔案辦理移交完畢後，應由移交人、接交人及監交人共同於移交清冊簽章。移交清冊至少包含移轉之原因、對象、方法、時間、地點及移轉對象得保有該項個人資料檔案之合法依據與證明等，一式二份，由移交人、接交人各保存一份。

三、移轉前，應先行確認公司與當事人間之契約對於契約關係移轉規定。

如契約關係約定公司通知當事人後即得移交所蒐集、處理、利用之個人資料，則公司不必事先取得當事人書面同意，於通知當事人後即可予以移交其個人資料。

如契約關係之移轉並無上開規定，依民法規定，契約關係移轉應得當事人之同意。經當事人同意，且公司明確告知當事人移交之原因、對象、方法、時間、地點及移轉對象得保有該項個

人資料檔案之合法依據與證明後，方能移交其個人資料予受讓公司。

四、若當事人表示不同意該契約關係之移轉，公司應協助當事人進行解除契約關係程序，或依當事人請求刪除其個人資料，不得將該個人資料移交予受讓公司。

第八十九條　對業務終止應遵循之程序

一部或全部業務終止，應遵循以下程序。

一、應盤點該終止業務之相關個人資料檔案，並造冊管理。

二、應主動於業務終止前，於告知當事人後，刪除所保有之個人資料檔案。如當事人提出異議者，得依當事人請求進行該個人資料檔案之後續處理。

第九十條　檔案銷毀或移轉

個人資料檔案銷毀或移轉，應依法令及內部規定之保存年限保留銷毀或移轉相關紀錄。

第二十四章　個人資料保護管理教育訓練

第九十一條　教育訓練

人力資源單位每年應透過 E-Learning 或其他方式對金控及子孫公司施以「個人資料保護法因應與衝擊認知教育訓練」，並留存紀錄。對新進人員個人資料保護法之教育訓練併入新進人員訓練課程。

第九十二條　依業務性質規劃之教育訓練

為使執行業務過程中必須接觸個人資料之人員(包括公司之定期或不定期契約人員及派遣員工)瞭解個人資料保護相關法令之要求、個人資料保護管理之重要性、使用個人資料應承擔之責任、違反個人資料保護管理對公司及行為人之影響、各種個人資料保護事項之機制、程序、措施及落實執行對客戶資料保密之義務，公司每年應依照業務之性質規劃年度個人資料保護管理教育訓練，並留存軌跡。

第九十三條　教育訓練內容之檢視

因應公司經營環境變遷、法規之變動，至少每年檢視個人資料保護管理教育訓練內容之妥適性。

第二十五章　稽核及改善程序

第九十四條　內部稽核及內部自行查核

本辦法管理機制應納入內部稽核及內部自行查核範圍，以檢視本辦法之有效性及落實執行情形。

第九十五條　內部稽核及內部自行查核缺失之追蹤及改善

內部稽核及內部自行查核所發現之缺失，業務單位應加強辦理改善及擬訂預防措施，並追蹤至完成改善為止。

第二十六章　其他

第九十六條　核決權限

本辦法所言之主管簽核、核准、核閱或書面同意，依各單位內部分層負責決行。

第九十七條　例外管理

如因業務特性或成本考量，無法符合本辦法之規定，應先行評估風險可接受程度，並規劃相關補償性措施，在符合個資法相關法令規範前提下，得以簽呈方式，呈所屬公司總經理取得例外管理之核可。

第九十八條　細部規章之建立

各單位得依業務特性建立更為細部之標準作業程序或修訂既有規範。

第九十九條　本辦法之定期檢視

本辦法至少每年檢視一次，以反應個人資料保護相關法令、技術及業務最新發展現況，並確保個人資料安全維護作業之有效性。

第一百條　個資侵害事故之緊急應變計畫演練

本公司及子公司應至少每年執行個資侵害事故之緊急應變計畫演練作業，並留存相關紀錄以供備查。

第一百零一條　附則

其餘未盡事宜，悉依主管機關相關法令及本公司相關規範辦理。

第一百零二條　施行及修訂

本辦法經本公司總經理核定並依本公司「章則制定政策」公告施行，修訂時亦同。

富邦金控

附表：改版紀錄

版次	核准日期	生效日期	核定層級	備註
01	2012/10/04	--	總經理	
02	2013/12/03	--	總經理	
03	2014/03/31	--	總經理	
04	2015/09/10	--	總經理	
05	2016/04/18	--	總經理	
06	2017/04/06	--	總經理	
07	2019/05/19	2019/05/27	總經理	
08	2019/10/23	2019/10/31	風險控管處處長	本次修正未涉及實質變更，依本公司「章則制定政策」，授權風險控管處處長核定
09	2020/07/22	2020/07/30	風險控管處處長	本次修正未涉及實質變更，依本公司「章則制定政策」，授權風險控管處處長核定
10	2022/03/10	2022/03/18	總經理	
11	2023/04/13	2023/04/14	風險控管處處長	依據本公司「章則制定政策」第三條第二項修正，未涉及實質變更所為之修訂

附件一

個人資料侵害事故通報表		
事件發生時間		
事件發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故	個資侵害之總筆數(大約) _____ □一般個資 _____筆 □特種個資 _____筆
發生原因及事件摘要		
損害狀況		
個資外洩可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩當日通報作業風險暨綜合規劃部	□是　□否，理由	

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。

事件發生單位或權責單位：

主管：　　覆核：　　經辦：

金 控 風險控管處簽收：　年　月　日　時　分

金 控 稽 核 處 簽 收：　年　月　日　時　分

富邦金控

附件二

<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
_____</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小時通報金管會</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 小時通報金管會，例假日均納入時效計算。