

中信保全股份有限公司

個人資料檔案安全維護管理辦法

第一章 總則

第一條 中信保全股份有限公司（以下簡稱「本公司」）為維護個人資料檔案安全，防止個人資料遭竊取、竄改、毀損、滅失或洩漏，特訂定「中信保全股份有限公司個人資料檔案安全維護管理辦法」（以下簡稱「本辦法」），俾利遵循。

第二條 本辦法係依據「個人資料保護法」第二十七條第三項及「內政部指定警政類非公務機關個人資料檔案安全維護管理辦法」制定。

第三條 本辦法用詞，定義如下：

- 一、 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
- 二、 蒐集：指以任何方式取得個人資料。
- 三、 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
- 四、 利用：指將蒐集之個人資料為處理以外之使用。
- 五、 國際傳輸：指將個人資料作跨國（境）之處理或利用。
- 六、 當事人：指個人資料之本人。
- 七、 個人資料事故：指個人資料遭竊取、竄改、毀損、滅失或洩漏之情形。
- 八、 重大個人資料事故：指個人資料遭竊取、竄改、毀損、滅失或洩漏達五千筆以上之情形。
- 九、 主管機關：為台北市政府警察局。

十、中央主管機關：為內政部警政署。

第二章 個人資料檔案安全維護計畫

第四條 本公司行政部編制檔案維護主管一名、檔案管理員一名，負責規劃、訂定、修正及執行個人資料檔案安全維護計畫及業務終止後之個人資料安全處理等相關事項，並定期向董事長提出報告。

本公司各單位主管為單位內個人資料檔案維護及管理工作的負責人員，應遵循個人資料保護相關法令、本公司「個人資料保護管理政策」及本辦法規定，並配合行政部協助執行個人資料檔案安全維護計畫及業務終止後之個人資料安全處理等相關事項，以確保落實個人資料保護機制。

第五條 本公司蒐集、處理及利用個人資料範圍：

- 一、 資料蒐集與利用之目的：保全服務契約、客戶管理與服務、人事管理、採購管理。
- 二、 客戶個人資料：指客戶之姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式及其他得以直接或間接方式識別該個人之資料。
- 三、 面試人員與員工個人資料：指面試人員與員工之姓名、出生年月日、身分證統一編號、婚姻、家庭、職業、健康檢查、財產狀況、聯絡方式等，及其他得以直接或間接識別該個人之資料。

第六條 本公司依據「個人資料管理政策」，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於營業處所之公佈欄，並揭露於網站首頁，俾使所屬人員及個人資料當事人均能知悉。

第七條 本公司各單位應每年清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或為其他適當之處置，檔案管理員並應留存相關紀錄。

第八條 本公司倘發生個人資料事故時，應依下列程序辦理：

- 一、單位於個人資料事故發生後，應通知檔案管理員及檔案維護主管，並儘速研議應變措施，以控制事故對當事人之損害，檔案管理員及檔案維護主管並將調查結果、因應措施及檢討報告（含矯正預防措施）呈報董事長。
- 二、檔案維護主管於接獲單位之通知後，應判斷是否屬於重大個人資料事故，如屬重大個人資料事故，應依第二項規定通報主管機關。
- 三、確認個人資料事故之當事人後，單位主管應以適當方式通知當事人。通知當事人事項應至少包括事故事實、所為因應措施及諮詢服務專線等內容。

本公司倘發生重大個人資料事故時，應依「內政部指定警政類非公務機關個人資料檔案安全維護管理辦法」第八條附件之格式於發現後七十二小時內以書面通報主管機關，並副知中央主管機關。

第九條 本公司各單位為執行業務而蒐集、處理個人資料時，應檢視是否符合「個人資料保護法」第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合「個人資料保護法」第二十條第一項但書情形。

第十條 本公司各單位蒐集個人資料，應遵守「個人資料保護法」第八條及第九條有關告知義務之規定。

本公司各單位直接向當事人蒐集個人資料時，應明確告知當事人下列事項：

- 一、公司名稱。
- 二、蒐集目的。
- 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、當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。
- 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。

本公司各單位所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前項應告知之事項。

第十一條 中央主管機關依「個人資料保護法」第二十一條規定對本公司為限制國際傳輸個人資料之命令或處分時，本公司行政部應通知各單位人員遵循辦理。

本公司各單位將個人資料作國際傳輸前，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：

- 一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。
- 二、當事人行使「個人資料保護法」第三條所定權利之相關事項。

第十二條 本公司於個人資料當事人行使「個人資料保護法」第三條規定之權利時，應依下列規定辦理：

- 一、提供聯絡窗口及聯絡方式。
- 二、確認為個人資料當事人之本人，或經其委託者。

三、認有「個人資料保護法」第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由，應檢附理由通知當事人。

四、有收取必要成本費用者，應告知當事人收費基準。

五、遵守「個人資料保護法」第十三條有關處理期限規定。

第十三條 本公司對所蒐集保管之個人資料檔案，應採取必要適當之資料安全管理措施。

前項資料安全管理措施，應包含下列事項：

一、紙本資料之控管：

(一) 對於各類契約書之調閱或其他管理，應依本公司「契約管理政策」相關規定辦理。

(二) 對於各類個人資料，應指定專人管理並存放於公文櫃或檔案室內並上鎖，非經單位主管同意不得任意複製或影印。

(三) 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

二、電腦存取個人資料之控管：

(一) 個人資料檔案儲存在電腦硬式磁碟機上者，應於個人電腦設置識別密碼、保護程式密碼或相關安全措施。

(二) 個人資料檔案使用完畢應即關閉，不得任其停留於電腦螢幕上。

(三) 定期進行電腦系統防毒、掃毒之必要措施。

(四) 重要個人資料應另加設密碼管控及傳輸。

第十四條 本公司為確實保護個人資料之安全，對人員應採取適度管理措施。

前項人員管理措施，應包含下列事項：

- 一、各單位依據業務需求，適度設定所屬人員（主管、非主管人員）不同之權限，以控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。
- 二、各單位應妥善保管個人資料及儲存媒介物，執行業務時依「個人資料保護法」規定蒐集、處理及利用個人資料。
- 三、單位所屬人員職務異動時，應將所保管之個人資料及儲存媒介物移交。
- 四、單位所屬人員離職時，應刪除該離職人員之電腦權限，並就其執行業務所持有之個人資料及儲存媒介物辦理交接，不得在外繼續使用，並應簽訂保密切結書（如任職時之相關勞務契約已有所約定時，亦屬之）。
- 五、本公司與員工或客戶所簽訂之相關勞務契約或承攬契約均載明保密條款，以確保其遵守對於個人資料內容之保密義務。

第十五條 本公司為妥善保護個人資料之安全，應採取必要適當之設備安全管理措施。

前項設備安全措施，應包含下列事項：

- 一、建置個人資料之電腦、自動化機器相關設備、可攜式設備，於保養維護或更新設備時，應注意資料之備份及相關安全措施。
- 二、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。
- 三、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，應檢視該設備所儲存之個人資料是否確實刪除。如委託他人執行者，本公司應依「個人資料保護法施行細則」第八條規定對受託者為適當之監督，並與受託者明確約定監督事項及方式。

第十六條 本公司如遇使用資通訊系統蒐集、處理或利用客戶個人資料達五千筆以上者，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、個人資料檔案及資料庫之存取控制與保護監控措施。
- 五、防止外部網路入侵對策。
- 六、非法或異常使用行為之監控與因應機制。

前項第五款及第六款所定措施，應定期（兩年一次）演練及檢討改善

第十七條 本公司如因解散、歇業、公司合併或其他原因終止業務後，不得繼續使用所保有之個人資料，並依實際情形採下列方式處理，並留存相關紀錄，其保存期限至少五年：

- 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
- 二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
- 三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第十八條 本公司各單位執行本辦法所定各種個人資料保護機制、程序及措施，應記錄個人資料使用狀況，並留存軌跡資料或其他相關之證據資料。

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、時間或地點。

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、地點，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。

第三章 附則

第十九條 本公司行政部對於個人資料蒐集、處理及利用，應定期或不定期對於各單位施以基礎認知宣導或教育訓練，俾使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

第二十條 本公司行政部應每半年至少進行一次個人資料檔案安全維護計畫及業務終止後個人資料處理方法執行情形之查核，且就查核結果向董事長提出報告，並留存相關紀錄，其保存期限至少五年。

前項檢查結果發現個人資料檔案安全維護計畫及業務終止後個人資料處理方法不符法令或有不符法令之虞者，本公司相關單位應研提改善措施並確保相關措施之執行。

第二十一條 本公司應適時參酌業務及個人資料檔案安全維護計畫執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討本辦法，必要時應予修正；修正後，應於十五日內將修正後之本辦法報請主管機關備查。

第二十二條 本公司倘因業務需要委託他人蒐集、處理或利用個人資料之全部或一部份時，應依「個人資料保護法施行細則」第八條規定為適當監督並與受託者明確約定相關監督事項及方式。

第二十三條 本辦法如有未盡事宜，悉依個人資料保護相關法令規定辦理。

第二十四條 本辦法經董事長核准後公告施行；修正時，亦同。

資安等級：內部

解密日期：9999

制定/修訂紀錄：

105年11月24日制訂

111年04月25日修訂