

中信保全股份有限公司

保全業個人資料檔案安全維護管理辦法

105.12.16

- 第一條 本辦法係依據內政部於105年7月8日所頒布之台警字第1050890353號「保全業個人資料檔案安全維護管理辦法」辦理之（以下簡稱本辦法），並依「個人資料保護法」第二十七條第三項規定訂定之。
- 第二條 本法主管機關為台北市政府警察局。
- 第三條 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，特依據內政部所令頒之「個人資料檔案安全維護管理辦法」，訂定本公司之個人資料檔案安全管理辦法，以防止員工個人資料遭竊取、竄改、毀損或洩漏。
- 第四條 本公司就現有員工之個人資料集中由行政部統一集中保管，並各事業部門將個人資料予以分類保管，並設置專櫃儲存；有關安全維護管理依據內政部所頒「保全業個人資料檔案安全維護管理辦法」第六條至第二十二條規定，訂定適當之安全維護管理措施，本計畫包括如后：
- 一、組織規模方面：本公司設置行政部門，編制人事檔案員乙位、總務人員乙位以協助人事檔案員就個人資料方面予以整理。
 - 二、個人資料檔案安全管理措施部份如下：
 - （一）個人資料檔案除配置人事、總務各乙人外，並由單位主管負責審查及簽核。
 - （二）錄取之員工個人資料（包含家庭狀況、連絡電話、身份背景等）由人事檔案員將個人資料建立人事電腦系統內，並分類各事業部門人資，俾利檔案管理。

- (三) 各勤務主管應落實員工考核、職前及在職教育訓練，對於員工於工作期間若有不適任者，應即反應人事部門。
- (四) 對於員工在案場違反工作紀律者，如侵佔財務、性騷擾女性住戶等等，勤務主管應即反映公司，並由主管召開會議，以採取因應作為。
- (五) 個人資料之蒐集、處理勤務主管應確實注重保密，嚴禁對非相關人員洩漏個資
- (六) 設備安全暨資料安全管理，統由負責人事之人員負責檔案人員管理，並由單位主管稽核。
- (七) 人事（檔案）管理人員需確實遵守本辦法規定，嚴禁對非相關人員透漏員工個人資料，若有洩漏個資之情形，將依個人資料保護法第 41 條規定辦理。
- (八) 個人資料安全維護稽核，每季由單位主管查察，以落實個人資料檔案安全管理。
- (九) 人事（檔案）管理人員，將員工之資料存檔於人資系統後，應建立備份資料，離職員工應另設資料存檔，以保存證據。
- (十) 個人資料安全維護之整體作業及規劃，人事系統檔案需建立密碼，除承辦人員使用外，任何人不得任意操作，檔案人員應定期及不定期應審查有無缺失，一經發現有作業上之問題，應即採取因應作為，以防堵資料外洩之情形。
- (十一) 業務終止後之個人資料之處理，統一造冊登錄後銷毀，並由單位主管監督。

第五條 本法經律訂後報請主管機關台北市政府警察局備查。

第六條 本公司辦理本法配置人事（檔案）管理人員，並由單位主管負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。

本公司依據個人資料保護管理之政策，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，公告於公佈欄內，並用公司網站揭露於網站首頁，使所屬人員及個人資料當事人均能知悉。

第七條 本公司在對於個人之彙整及處理及利用個人資料之類別及範圍，每季清查所保有個人資料檔案之現況。

依前項清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，人事（檔案）管人員並應留存相關紀錄。

第八條 本公司在界定蒐集、處理與利用個人資料之類別、範圍及流程，分析評估可能發生之風險，擬訂定適當之管控措施，以杜絕個人資料外洩情事發生。

第九條 倘發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應即採取應變機制，作法應包括下列事項：

一、對於造成當事人之個資外洩，除應即查明原因及追究承辦人員外，並即通知當事人，以減少對當事人之損害。

二、對於事故發生原因及損害狀況，除採取因應防堵措施外，並責由單位主管給予諮詢服務及專線。

三、造成個人資料洩漏人事（檔案）管理人員，應研議改進措施，避免類似事故再度發生。

四、發生重大個人資料事故者，應即以書面通報主管機關。

前項第四款所稱重大個人資料事故，指個人資料被竊取、洩漏、竄改或其他侵害事故，致危及大量當事人權益之情形。

第十條 本公司勤務主管及人事（檔案）管理人員，為執行業務蒐集個人資料時，應檢視符合蒐集要件及特定目的之必要範圍，並接受單位主管之監督。

第十一條 本公司在蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求勤務主管及人事（檔案）管理人員確實辦理。

第十二條 依據中央主管機關依本法第二十一條規定「對保全業為限制國際傳輸個人資料之命令或處分時，本公司應通知勤務主管及人事（檔案）管理人員遵循辦理。

第十三條 本公司所蒐集之個人資料需作特定目的外利用者，應檢視有無本法第二十條第一項但書規定得為利用之情形。

第十四條 本公司於個人資料當事人行使本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、認有本法第十條但書各款、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、收取必要成本費用者，應告知當事人收費基準。
- 五、遵守本法第十三條有關處理期限規定。

第十五條 本公司對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。

前項安全設備或防護措施，應包含下列事項：

- 一、紙本資料檔案之安全保護設施。

- 二、電子資料檔案存放之電腦、可攜式設備或儲存媒體，配置安全防護系統或加密機制。
- 三、存有個人資料之紙本、磁碟、光碟片、或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料。

第十六條 本公司為確實保護個人資料之安全，對勤務主管、人事（檔案）管理人員應採取適度管理措施。

前項管理措施，應包含下列事項：

- 一、依據業務需求，適度設定所屬人員不同之權限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、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
- 三、勤務主管、人事（檔案）管理人員，應確實妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
- 四、勤務主管及人事（檔案）管理人員離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

第十七條 本公司對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條相關規定，並定期或不定期對於所屬人員施以基礎認知宣導或專業教育訓練，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。

第十八條 本公司應訂定個人資料檔案安全維護稽核機制，每半年定期或不定期檢查計畫執行情形，檢查結果並應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。

前項經主管機關檢查結果發現計畫不符法令或不符政府令之虞者，本公司應即改善。

第十九條 本公司應採行適當措施，留存個人資料使用紀錄、或其他相關之證據資料，其保存期限至少五年。

第二十條 本公司應隨時參酌業務及計畫執行狀況，社會輿情、及相關法規訂修等因素，檢討所訂定計畫，必要時應予修正；修正後，應於十五日內將修正計畫報請台北市政府警察局備查。

第二十一條 保全業務終止後，保有之個人資料不得繼續使用，應依下列方式處理，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，應依本法施行細則第八條規定為適當監督。

第二十三條 本辦法董事長核准後施行。