台灣華庫股份有限公司

個人資料檔案安全維護計畫

一、 個人資料保護政策

(一)個人資料保護法第 27 條第 3 項規定及移民業務機構個人資料檔案安全維護管理辦法規定辦理。

(二)本計畫目的，為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本公司人員應依本計畫辦理個人資料檔案安全管理維護。

二、 個人資料檔案之安全維護管理措施

(一) 配置管理之人員及相當資源

1. 配置管理人員：2 人。
2. 職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項。

(二) 界定蒐集、處理及利用個人資料之範圍

1. 特定目的：本公司個人資料蒐集、處理及利用之範圍，為入出國及移民、遊留學之業務，包括契約相關文書、法律關係事務、客戶管理與服務、護照、簽證及文件證明處理、諮詢與顧問服務，其他經營合於營業登記項目或組織章程所訂之業務、及本公司人事管理與依法辦理之員工健康檢查。
2. 資料類別：識別類、特徵類、家庭情形、社會情況、教育技術、受雇情形、財務細節、商業資訊、健康與其他、其他各類資訊。
3. 客戶個人資料：指本公司依前項特定目的之需求，蒐集客戶之個人資料，包含姓名、國民身分證統一編號、護照號碼、聯絡方式及其他得以直接或間接方式識別該個人之資料。
4. 所屬人員個人資料：指本公司依前項特定目的之需求，蒐集所屬人員之人事管理、教育訓練、依法辦理之員工健康檢查等個人資料，包含姓名、出生年月日、國民身分證統一編號、護照號碼、婚姻、家庭、教育、職業、健康檢查、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) 個人資料之風險評估及管理機制。

1. 風險評估：

(1) 經由本公司電腦下載或外部網路入侵而外洩。

(2) 經由書面資料外洩。

(3) 員工及第三人古意竊取、竄改、毀損或洩漏。

2. 管理機制：

(1) 藉由使用者代碼、識別密碼設定及文件妥適保管。

(2) 定期進行網路資訊安全維護控管。

(3) 加強員工管制教育訓練及設備強化管理。

(四) 個人資料蒐集、處理及利用之內部管理程序。

1. 本公司依前條個人資料蒐集之特定目的及必要性，蒐集、處理及利用個人資料，並定期清查所保有之個人資料現況。
2. 本公司所屬人員為執行業務所蒐集或委託他人蒐集之個人資料，均視為本公司所蒐集持有，並接受監督。
3. 本公司委託他人蒐集、處理或利用個人資料之全部或一部時，本公司應對受託者為適當之監督並與其明確約定相關監督事項。
4. 本公司指定之專責人員定期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個人資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。
5. 本公司所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合個人資料保護法之規定。
6. 進行個人資料國際傳輸前，應檢視有無內政部依個人資料保護法之規定。
7. 當事人表示拒絕行銷或請求閱覽、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時。聯絡窗口為林書瑜；連絡電話：(02)2362-9978；電子郵件信箱：lins@twc-consultancy.com

(五) 事故之預防、通報及應變機制。

1. 發現個人資料遭竊取、竄改、毀損、滅失或洩漏事件時，立即向公司負責人或授權主管通報。
2. 立即查明事件發生原因、損害狀況及責任歸屬，並採取適當之措施，控制事件對當事人造成之損害。
3. 對於個人資料遭竊取之客戶，以適當方式通知當事人，說明本公司已採取之處理措施，及本公司所提供之諮詢服務專線。
4. 針對事件發生原因研議改進措施，避免事件再度發生。

(六) 設備安全管理、資料安全管理及人員管理措施。

1. 電腦個人資料存取

(1)儲存個人資料檔案之電腦設備，應設置使用者代碼(帳號)及識別密碼、螢幕保護程式密碼之登入及相關安全措施。

(2)本公司所屬人員如因其工作執掌相關而須輸出、輸入個人資料時，均須以其個人之使用者代碼(帳號)及識別密碼登入，同時在使用範圍及權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

(3)個人資料檔案使用完畢應即登出系統或關閉檔案，不得任其停留於電腦螢幕上。

(4)重要個人資料應另加設管控密碼，非經陳報所屬主管同意，並取得密碼者，不得存取。

(5)定期進行電腦系統防毒、掃毒、安全性更新等資訊安全措施。

(6)禁止使用私人可攜式電腦設備(例如筆記型電腦、平板電腦等)、儲存媒體(例如外接式硬式磁碟、光碟、隨身碟、記憶卡等)或行動裝置(例如行動電話等)儲存本公司所保有個人資料檔案。

2. 紙本個人資料保管

(1)對於各類委託書、契約書件(含個人資料表)應存放於公文櫃內並上鎖，所屬人員非經所屬主管同意不得任意複製或影印。

(2)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。

3. 人員權限管控

(1)本公司依業務需求，得適度設定所屬人員不同之權限，以控管其個人資料之存取。

(2)本公司所屬人員應定期變更識別密碼，並於變更識別密碼後始可繼續使用電腦。

(3)本公司所屬人員離職或終止僱傭或委任契約時，將立即取消其使用者代碼(帳號)及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書(如在任職時之相關勞務契約已有所約定時，亦屬之)。

(4)本公司所屬人員應妥善保管個人資料之儲存媒體，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。

(5)本公司所屬人員所簽訂之相關勞務契約或承攬契約均訂定保密條款及相關之違

約罰則，以確保其遵守對於個人資料內容之保密義務(含契約終止後)。

(七) 設備安全管控

1. 儲存個人資料檔案之電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。
2. 儲存個人資料檔案之電腦設備，不得直接作為公用電腦使用。
3. 儲存個人資料檔案之電腦設備、儲存媒體及資料檔案，應指派專責人員管理，非經所屬主管同意並作成紀錄，不得攜帶外出或拷貝複製。
4. 個人資料檔案應定期備份，重要個人資料備份應異地存放，並防止資料滅失或遭竊取。
5. 儲存個人資料檔案之電腦設備及儲存媒體需報廢、汰換或轉作其他用途時，所屬主管應檢視該電腦設備及儲存媒體所儲存之個人資料是否確實刪除或破壞。

(八) 使用紀錄、軌跡資料及證據保存。

1. 使用紀錄、軌跡資料及證據保存，包含個人資料使用及查詢紀錄、電腦設備之軌跡資料，應製作備份，保存於適當處所。

(九) 資料安全稽核機制。

1. 本公司每年定期辦理個人資料檔案安全維護稽核，以落實本計畫之執行，針對缺失及潛在之風險，應規劃改善及預防措施，並依下列方式辦理：
   (1)確認缺失及潛在風險之內容及發生原因。
   (2)提出改善及預防措施。
   (3)紀錄稽核情形及結果。
2. 前項稽核情形及結果應載入稽核報告中，公司負責人或授權主管須簽名確認，相關紀錄至少保存一年備查。
3. 針對個人資料檔案安全維護稽核結果不符合法令之虞者，規劃改善與預防措施。

(十) 認知宣導及教育訓練。

1. 本公司每年進行個人資料保護法相關教育訓練至少一次，使所屬人員知悉應遵守之

規定，課程資料及簽到名冊等相關紀錄，至少保存一年備查。

2. 教育訓練內容得以法規宣導、專題演講、網路影音等形式辦理。

3. 對新進人員應特別給予指導，務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。

(十一) 個人資料安全維護之整體持續改善。

本公司將隨時依據計畫執行狀況、技術發展及法令修正等，檢討本計畫是否合宜，並予必要之修正後，報請主管機關核備後實施。

(十二) 業務終止後之個人資料處理方法。

本公司業務終止後，所保有之個人資料不得繼續使用，應依下列方式處理，並留存相關文件、照相、錄影紀錄備查：

1. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

2. 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。

3. 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。

三、 本計畫公告於網站首頁(https://www.twc-consultancy.com/)，使其所屬人員及資料當事人均能知悉；本計畫修正時，亦同。

計畫訂定日期：2021/10/01

台灣華庫股份有限公司