三芝慈安園有限公司
個人資料檔案安全維護計畫

壹、組織及規模

一、組織型態：有限公司

二、經營型態：直營

三、資本總額：新台幣（下同）3,000,000 元

四、處所地址：臺北市中山區民權東路 2 段 164 號 1 樓

五、代表人：邵明斌

六、員工人數： 5 人

貳、個人資料檔案之安全維護管理措施

一、個資保護管理小組

(一)個資保護管理小組

1. 組織：

召集人、管理代表、事故管理分組、申訴管理分組、風險管理分組、教育訓練分組、法規諮詢分組、文件管制分組、稽核分組。

2. 職責：

各分組組長負責規劃、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，並向管理代表提出報告，並呈報召集人。

(二)預算：2 萬元

(三)個人資料保護管理政策：

遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、篡改、毀損、滅失或洩漏。

二、個人資料之範圍

(一)特定目的：

不動產服務、代理與代銷業務、契約或類似契約或其他法律關係事務、消費者客戶管理與服務、人事管理。

(二)客戶個人資料：

本計畫所稱之客戶個人資料，除係指客戶姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式外及其他得以直接或間接方式識別該個人之資料。

(三)員工或所屬經紀人員個人資料：

指姓名、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。

三、風險評估及管理機制

(一)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、經由接觸書面契約書類而外洩。

3、員工故意竊取、毀損或洩漏。

(二)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及控管。

3、電磁資料視實際需要以加密方式傳輸。

4、加強對員工之管制及設備之強化管理。

四、個人資料蒐集、處理及利用之內部管理措施

(一)直接向當事人蒐集個人資料時，應明確告知以下事項：

a. 公司名稱、加盟品牌名稱。

b. 蒐集目的。

c. 個人資料之類別。

d. 個人資料利用之期間、地區、對象及方式。

e. 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。

(二)所蒐集非由當事人(或客戶)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。

(三)客戶洽詢物件階段，如獲得客戶書面同意，得進行個人資料蒐集、處理及利用。於銷售期限屆滿時應主動刪除或銷毀。但因執行業務所必須或經客戶書面同意者，不在此限。

(四)利用個人資料為行銷時，當事人（或客戶）表示拒絕行銷後，應立即停止利用其個人資料行銷。

(五)客戶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，來電客服人員，總公司電話 02-7726-5678 或客服電話 0800-002288。並將聯絡電話等資料，揭示於本公司營業處所或公司網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

(六)負責保管及處理個人資料檔案之人員，其職務有異動時，應將所保管之儲存媒體及有關資料檔案移交，以利管理

(七)本公司員工或所屬之經紀人員如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

(八)由指定之管理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。

(九)本公司如有委託他人（或他公司）蒐集、處理或利用個人資料時，應對受託者為適當之監督並與其明確約定相關監督事項。

(十)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規定。

(十一)本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

五、事故之預防、通報及應變機制

(一)預防：

1、本公司員工或所屬之經紀人員如因其工作執掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

2、非承辦之經紀人員參閱契約書類時應得公司負責人或經指定之管理人員之同意。

3、加強員工教育宣導，並嚴加管制。

(二)通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2、對於個人資料遭竊取之客戶，以書面通知使其知悉及本公司已採取之處理措施。

3、針對事故發生原因研議改進措施。

六、資料安全管理、人員管理及設備安全管理

（一）資料安全管理

1、電腦存取個人資料之管控：

（1）個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）本公司員工或所屬經紀人員如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，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退出，不得任其停留於電腦終端機上。

（4）定期進行電腦系統防毒、掃毒之必要措施。

（5）重要個人資料應另加設管控密碼，非經陳報單位主管核可，並取得密碼者，不得存取。

2、紙本資料之保管：

（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，員工或所屬經紀人員非經公司負責人或營業處所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。

（二）人員管理

1、本公司依業務需求，得適度設定所屬人員(例如主管、非主管人員)不同之權限，以控管其個人資料之情形。

2、本公司員工或所屬之經紀人員每 3 個月應變更識別密碼 1 次，並於變更識別密碼後始可繼續使用電腦。

3、員工離職或所屬之經紀人員與公司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、本公司員工及所屬經紀人員應妥善保管個人資料之儲存媒介物，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。

5、本公司與員工或所屬之經紀人員所簽訂之相關勞務契約或承攬契約均列入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）。

（三）、設備安全管理

1、建置個人資料之有關電腦設備，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、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。

3、公司應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。

4、本公司之客戶個人資料檔案應定期下載以作為備份。

5、重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止資料滅失或遭竊取。

6、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，本公司負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除。

七、資料安全稽核機制

(一)本公司定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1.確認不符合事項之內容及發生原因。

2.提出改善及預防措施方案。

3.紀錄查察情形及結果。

(二)前項查察情形及結果應載入稽核報告中，由召集人須簽名確認。

八、使用記錄、軌跡資料及證據保存

(一)紙本資料

1.紙本資料除依據「文件管理辦法」進行實體存取之安全管控外，大量紙本保存時應注意該紙本事後檢索、取回(retrieve)之可能性及作業方式，以因應當事人提出刪除之請求。

2.紙本之存放應注意防潮及防火，避免意外毀損。

3.紙本存放之倉庫，應注意其安全性，如與其他物品共置於一室，應透過監視(Surveillance)防護措施，或其他安全管制措施(例如人員陪同)進行存取控制防護。

(二)電子資料(存放於電腦或伺服器)

1.存放於個人電腦者

(1)電子(檔案、資料庫等)型態之個人資料存放於個人電腦時，應裝設防毒軟體，嚴禁使用 P2P 類型之高風險軟體。

(2)電子型態之個人資料存放於個人電腦，應確保僅存放最少之需求資料，以避免過多資料存放之風險。

(3)稽核分組應於稽核時進行個人電腦之檢核，確保個人電腦未存放非業務需求之個人資料檔案。

(4)經常性存放個資於個人電腦者，應事先進行申請，由該部門主管及該資料業管單位進行審核，確保該電腦有足夠安全防護。

(5)個人資料存放於個人電腦，必要時應進行資料之加密，以降低資料遭竊取、遺失之風險。

2.存放於電腦伺服器者

(1)嚴禁以未有存取控制之方式進行檔案共享。

(2)檔案伺服器之存取權限應視需求開放，並定期檢視其存取權限之設定。

(3)檔案伺服器之管理者權限應控制其必要數量，避免過多的管理者權限可存取非業務相關之資料檔案。

(4)存放於檔案伺服器中之檔案，應視需求定期進行檢視，確保其存放之安全防護需求。

(5)高重要性或大量個人資料存放之檔案應視需求進行加密作業，以避免個資洩漏、遺失之風險。

(6)檔案伺服器應留存相關存取紀錄，並由管理人員定期檢視是否有異常之存取行為。

(三)資料儲存媒體

1.可移除式媒體

未經核准不應使用可移除式硬碟機進行個人資料之複製或備份。

2.磁帶媒體(Tape, CD, DVD…)

儲存個人資料檔案之媒體應依據相關作業規範對於媒體之管制作業進行控管。

九、認知宣導及教育訓練

(一)本公司每年進行個人資料保護法基礎教育宣導及教育訓練至少 1 次，使員工或所屬之經紀人員知悉應遵守之規定。前述教育宣導及訓練應留存紀錄（例如：簽名冊等文件）

(二)對於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、個人資料安全維護之整體持續改善

(一)本公司將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

(二)針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十一、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，依下列方式處理，並留存相關紀錄：

(一)該個人資料若超過保存期限，不予保留而須進行銷毀時，應由各部室主管填寫「銷毀申請單」，依審查核准後，以碎紙機絞碎或撕毀等無法回復之安全方式處理。

(二)若委外執行銷毀，各部室主管應會同稽核員監視銷毀流程，留存相關紀錄並附於「銷毀申請單」以供備查。

(三)「銷毀申請單」應由文件管制人員永久保存。