龍巖股份有限公司

一、目的

（一）本辦法依「個人資料保護法」(以下簡稱個資法)第二十七條第三項暨「殯葬服務業個人資料檔案安全維護管理辦法」(以下簡稱殯服業個資安全法)第三條訂定之。

（二）落實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、滅失或遺漏。

二、範圍/制定機關

（一）本公司所有與個人資料相關之營運流程。

（二）本公司及子公司全體員工。

（三）承攬本公司業務之公司單位及個人。

（四）與本公司所有合作之廠商與個人暨其複委託之廠商或個人。

（五）本公司客戶。

（六）委託本公司蒐集、處理或利用個人資料之外部機關或個人。

（七）本辦法之制定機關為客戶服務部。

三、參考文件

（一）個人資料保護法。

（二）殯葬服務業個人資料檔案安全維護管理辦法。

（三）殯葬服務業個人資料檔案安全維護計畫範本。

四、定義

（一）本辦法用詞，定義如下：

1、個人資料：依個資法第2 條第一款所稱個人資料及個資法第2 條第二款所稱之個人資料檔案。

2、資料管理單位(或稱權責單位)：為所屬業務與因業務執行而進行資料蒐集、處理、利用資料之業務執行單位。

3、權責單位：指本公司得查詢、運用個資之所有單位。

4、個資管理單位：為客戶服務部。

五、權責

（一）董事長或經其授權之經理部門：個人資料處理方法之訂定、審查、修正。

（二）客服部：定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。遇有重大個人資料安全事故者，依應通報總經理並依本公司「營運程序異常事件處理辦法」執行相關事項。

（三）權責單位：單位內個人資料損害預防及危機處理應變之通報。

（四）稽核室：定期或不定期將相關機制列入內部控制及稽核項目。

六、關鍵管理

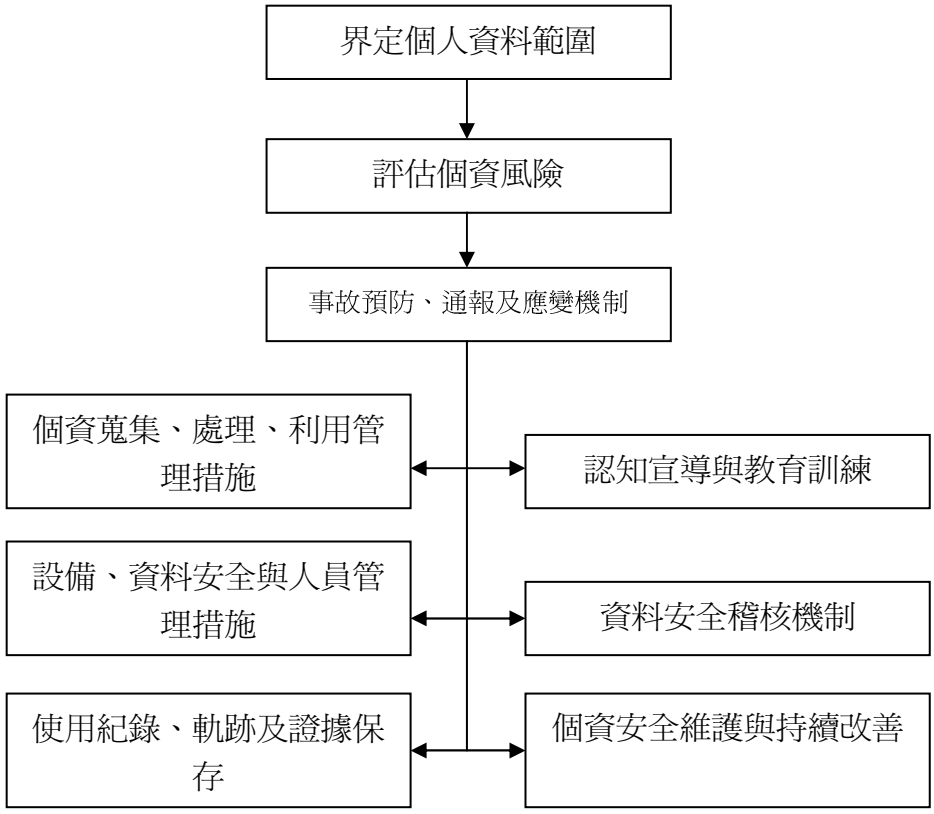
（一）關鍵管理項目

1、界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管理機制。

2、因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，應訂定應變、通報及預防機制。

3、個人資料之安全稽核、紀錄保存及持續改善機制。

（二）關鍵管理程序圖



七、公司組織規模

（一）組織型態：股份有限公司

（二）營業項目：殯葬設施經營業暨殯葬禮儀服務業

（三）資本額：6,000,000,000 元

（四）公司地址：臺北市中山區民權東路 2 段 166 號 1 樓

（五）代表人：李世聰

（六）員工人數：450～500 人

八、修正歷程

（一）本辦法於民國一○三年十二月二十六日經董事長核准通過，並自公告日起施行之。

（二）本辦法於民國一○五年一月二十九日修訂,經董事長核准通過，並自公告日起施行之。

九、附件

（一）個人資料檔案之安全維護管理措施(附件一)

附件一:個人資料檔案之安全維護管理措施

一、管理人員與資源配置

（一）管理人員：

1、配置人數：1 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）預算：每年約 80 萬～100 萬。

二、界定蒐集、處理及利用個人資料之範圍

（一）特定目的：人事管理、行銷、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、消費者保護、廣告或商業行為管理。

（二）資料類別：

1、辨識個人者：如客戶及員工之姓名、地址、住家及行動電話號碼、電子郵件及其他任何可辨識資料本人者等資訊。

2、辨識財務者：如信用卡號碼或金融機構帳戶資訊。

3、個人描述：如性別、出生年月日等。

三、風險評估及管理機制

（一）風險評估

1、經由本公司或各營業處所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、本公司與各營業處所間或依殯葬管理條例第五十六條規定受委託之公司或商業間互為傳輸時外洩。

4、員工故意竊取、竄改、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、事故之預防、通報及應變機制

（一）預防：

1、本公司員工如因工作執掌而須輸出、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、非承辦之人員參閱契約書類時應取得權責單位主管或經指定之管理人員之同意。

3、個人資料於本公司與各營業處所間或受委託之公司或商業間互為傳輸時，加強管控避免外洩。

4、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、滅失或洩漏應立即向權責主管與個資管理單位通報，並立即查明發生原因及責任歸屬，依實際狀況採取必要措施降低對客戶、公司之影響。

2、對於個人資料遭竊取之客戶，應儘速以適當方式通知使其知悉，並告知本公司已採取之處理措施及聯絡電話窗口等資訊。

3、事故發生之單位應針對事故發生原因研議並於事故發生日起 30 天內提出改進措施，經個資管理單位審查後送事業群主管同意後執行之。

4、重大資安事故需通報至總經理，並依公司「營運程序異常事件處理辦法」執行相關事項，其後續所研議之再發防止措施，需經總經理同意後執行之。

5、重大資安事故定義：個人資料遭竊取、竄改、毀損、滅失或洩漏，已有危及公司正常營運或大量當事人權益之情形。

五、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：

1、公司名稱。

2、蒐集之目的。

3、個人資料之類別。

4、個人資料利用之期間、地區、對象及方式。

5、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。

6、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。

7、當事人請求製給複製本時，相關單位得收取手續費用，手續費用依當時公告辦理。

（二）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。

（三）與客戶簽訂之殯葬服務契約（含生前殯葬服務契約）完成履行、解除或終止時，除因執行業務所必須（有約定之保存期限、有理由足認刪除將侵害當事人值得保護之利益、其他不能刪除之正當事由）或經客戶書面同意者，應主動刪除或銷毀，並留存相關紀錄。

（四）各單位利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並將拒絕情形予以紀錄，個資管理單位必要時得將該資料予以禁止使用或銷毀。

（五）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，連絡窗口為：客戶服務部；電話為：0800-018-999。

（六）聯絡窗口及電話等資料，應公告於本公司及各營業處所，如有網站者，並揭露於網頁。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。

（七）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。

（八）員工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。

（九）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、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。

（十）本公司依殯葬管理條例第五十六條規定委託代為銷售生前殯葬服務契約、墓基及骨灰（骸）存放單位之公司，為執行業務所蒐集、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。

（十一）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第二十條第一項但書規定。

六、設備安全管理、資料安全管理及人員管理措施

（一）設備安全管理

1、建置個人資料之有關電腦、自動化機器相關設備、可攜式設備，資訊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、客戶個人資料檔案應定期備份。

4、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。

5、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，權責單位主管、各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。

（二）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）個人資料檔案使用完畢應即退出，不得任其停留於電腦螢幕上。

（3）定期進行電腦系統防毒、掃毒之必要措施。

（4）重要個人資料應另加設管控密碼，並定期更換密碼，非經權責單位主管、各營業處所主管或經指定之管理人員核可，並取得密碼者，不得存取。

2、紙本資料之保管：

（1）對於各類契約書件及個人資料表應存放於公文櫃內並上鎖，員工非經權責單位主管、各營業處所主管或經指定之管理人員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。

（三）人員管理措施

1、員工需依其業務、職務需求設定不同之權限，以控管其個人資料蒐集、處理與利用之情形。

2、個資管理單位應檢視各相關業務之性質，指派人員負責規範個人資料蒐集、處理及利用等流程。

3、員工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。

4、員工離職應立即取消其使用者代碼及識別密碼。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。

5、員工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，保密義務期限包含至契約終止後。

6、員工電腦設備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。

7、員工使用紙本個人資料應隨時收藏整理，未用時應存放於櫃內並上鎖，不得任意放置於桌上或第三人可以任意取得之處。

七、認知宣導及教育訓練

（一）個資管理單位應進行個人資料保護法基礎認知宣導及教育訓練，或得派遣員工參與相關單位辦理進行個人資料保護法基礎教育宣導及數位學習教育訓練，使員工知悉應遵守之規定，前述教育宣導及訓練應留存紀錄。

（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。

八、資料安全稽核機制

（一）稽核單位應至少每兩年需辦理個人資料檔案安全維護稽核，查察個資使用單位是否落實本規範事項，針對查察結果不符合事項及潛在不符合之風險，應規劃改善與預防措施，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作成稽核報告，由相關單位主管簽名確認，稽核報告至少保存五年。

九、使用記錄、軌跡資料及證據保存

（一）公司建置個人資料之電腦，其個人資料使用查詢紀錄檔，每年定期備份加密，並將該紀錄檔之儲存媒介物保存於適當處所以供檢查。

（二）紙本個人資料之使用與調閱，於應以系統表單提出需求，非經權責單位主管、各營業處所主

管或經指定之管理人員同意，不得任意取出。

十、個人資料安全維護之整體持續改善

（一）個資管理之權責單位需隨時依據辦法執行狀況，技術發展及相關法令修正等事項，檢討本辦法是否合宜，並予必要之修正。

（二）稽核單位針對個資安全稽核結果有不符合法令之虞者，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

（一）公司業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄至少五年：

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。