**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(業者名稱)**

**個人資料檔案安全維護計畫**

**一、公司組織現況及人員配置**

（一）組織型態：有限公司/（股）公司／獨資

（二）營業項目：殯葬禮儀服務業

（三）資本額：新臺幣\_\_\_\_\_\_\_\_\_\_萬元整

（四）營業地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

（五）負責人：\_\_\_\_\_\_\_\_\_\_\_\_

（六）員工人數：\_\_\_\_\_\_人

（七）管理人員配置：\_\_\_\_\_\_\_人（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）

（八）預算：包含管理津貼、設備、材料費等每年新臺幣\_\_\_~\_\_\_萬元

**二、個資範圍及風險評估**

（一）個資範圍：

１、凡公司受理之殯葬服務案件，其過程所收取個人身分證件、相關證明文件、資料、戶籍謄本、戶口名簿、照片、文字或影音檔案、訂立殯葬契約內容等。

２、凡公司僱聘之員工個人資料及人事管理資料，或類似契約或其他法律關係事務、客戶申訴資料、客戶管理與服務資料、消費者保護、廣告或商業行為等。

３、資料類別包含：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。

（二）風險評估：

１、經由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、公司與各營業處所間或配合廠商或商業間互為傳輸時洩。

４、員工故意竊取、竄改、毁損或洩漏。

**三、預防、通報及應變機制**

（一）預防：

１、公司員工如因工作而須輸出、輸入個人資料時，均須鍵入其個人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資料時應經公司負責人或指定之管理人員同意。

３、個人資料於公司與各營業處所間或配合廠商或商業間互為傳輸時，應加強管控避免外洩。

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、滅失或洩漏等個人資料安全事故(參酌內政部指定殯葬服務業個人資料檔案安全維護管理辦法第十四條)，即向公司負責人或指定之管理人員通報，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。

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，並告知公司已採取之處理措施及聯絡電話窗口等資訊。

３、針對事故發生原因研議改進措施，而殯葬服務業遇有達一千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報直轄市、縣（市）主管機關，並副知中央主管機關（書面通報格式參酌內政部指定殯葬服務業個人資料檔案安全維護管理辦法第十四條附件）。

**四、內部管理機制**

本公司個資管理機制內涵包括：藉由使用者代碼、識別密碼設定及文件妥適保管；定期進行網路資訊安全維護及控管；電磁資料視實際需要以加密方式傳輸；加強對員工之管制及設備之強化管理。以下分列「個人資料蒐集、處理及利用之管理措施」、「設備安全管理措施」、「資料安全管理措施」、「人員管措施」四個項目：

|  |  |
| --- | --- |
| 項目類別 | 管理機制具體措施 |
| 個人資料蒐集、處理及利用之管理措施 | 1.直接向當事人蒐集個人資料時，應明確告知以下事項：公司名稱、蒐集之目的、個人資料之類別；個人資料利用之期間、地區、對象及方式；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；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。  2.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。  3.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或經客戶書面同意者，應主動刪除或銷毀，並留存相關紀錄。  4.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，並將拒絶情形通報本公司彙整後周知所屬各部門及員工。  5.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：\_\_\_\_\_\_\_\_\_\_\_；電話為：\_\_\_\_\_\_\_\_\_\_\_。並將聯絡窗口及電話等資料，公告於公司及各營業處所，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。  6.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。  7.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。  8.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。  9.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。 |
| 設備安全  第2頁 共5頁  管理措施 | 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.客戶個人資料檔案每個月定期備份。  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，負責人或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。 |
| 資料安全  管理措施 | 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，非經陳報本公司）負責人、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，員工非經負責人、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。 |
| 人 員  管理措施 | 1.依業務需求設定所屬人員不同之權限，以控管其個人資料蒐集、處理與利用之情形。  2.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（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。  5.公司與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（含契約終止後）。  6、公司員工每3個月應變更識別密碼ㄧ次，並於變更識別密碼後始可繼續使用電腦。 |

**五、員工教育訓練**

（一）公司每一年進行個人資料保護法基礎認知宣導及教育訓練至少一次，每年派遣員工\_\_\_\_人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至少\_\_\_\_\_小時，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）對於新進人員須特別給予指導，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。

（三）公司員工就職守則或教育訓練內應列入個資相關遵守規定，並要求員工恪守相關規定。

**六、資料使用保存與安全稽核機制**

（一）使用記錄及證據保存：

１、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。

２、個人資料使用紀錄以紙本登記者，應存放於公文櫃內並上鎖，非經負責人、各營業處所主管或經指定之管理人員同意，不得任意取出。

（二）資料安全稽核機制與後續改善

１、公司每2年辦理個人資料檔案安全維護稽核，查察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，立即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。查察情形及結果並作成稽核報告，由負責人或經指定之管理人員簽名確認，稽核報告至少保存五年。

２、殯葬服務業使用資通訊系統蒐集、處理或利用個人資料達一萬筆以上者，應採取下列資訊安全措施：

(1)使用者身分確認及保護機制。

(2)個人資料顯示之隱碼機制。

(3)網際網路傳輸之安全加密機制。

(4)個人資料檔案與資料庫之存取控制及保護監控措施。

(5)防止外部網路入侵對策。

(6)非法或異常使用行為之監控及因應機制。

(7)應定期演練及檢討改善。

３、公司將隨時依據計畫執行狀況，技術發展及相關法令修正等事項，檢討本計畫是否合宜，並予必要之修正。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。

４、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。

(請蓋大小章)

中華民國 年 月 日