

個人資料檔案安全維護計畫

訂定日期：中華民國____年____月____日

壹、依據：

個人資料保護法第 27 條第 3 項及內政部指定宗教團體個人資料檔案安全維護管理辦法第 4 條。

貳、目的：

落實個人資料檔案之安全維護及管理，防止被竊取、竄改、毀損、滅失或洩漏。

參、組織規模及特性

- 一、負責人：_____
- 二、主事務所地址：_____
- 三、所屬人員人數：約_____人(註：包括管理組織人員、職員、同工、志工、所屬傳教人員、信徒、會員)
- 四、保有個人資料數量：約_____筆
- 五、負責人聯絡電話：_____

肆、個人資料檔案之安全維護管理措施

一、配置管理之人員及資源

(一) 管理人員：

- 1、配置人數：_____人(至少 1 名)。
- 2、職責：負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並每_____年向負責人提出報告。

(二) 預算：經費依實際需要支出。

二、蒐集、處理及利用個人資料之範圍及特定目的

(一) 個人資料範圍：

指本寺廟蒐集、處理及利用之自然人姓名、出生年月日、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。

(二) 蒐集、處理及利用個人資料之特定目的：

- 1、人事管理。

- 2、宗教、非營利組織業務。
- 3、寺廟對監察人、管理委員會成員及其他成員名冊之內部管理。
- 4、社會服務或社會工作。
- 5、非公務機關依法定義務所進行個人資料之蒐集處理及利用
(註：如疫情期間信眾實聯制資料。)

三、個人資料之風險評估及管理機制

(一) 風險評估

- 1、經由本寺廟電腦下載或外部網路入侵而外洩。
- 2、經由接觸涉有個人資料之業務書件而外洩。
- 3、所屬人員或其他人竊取、毀損或洩漏。
- 4、與所屬單位、機構間互為傳輸時外洩。

(二) 管理機制

- 1、適度設定所屬人員權限，並妥適保管文件。
- 2、每____年進行網路資訊安全維護及控管。
- 3、電子檔案資料視實際需要加密。
- 4、加強對所屬人員及設備之管理。

四、事故之預防、通報及應變機制

(一) 預防：

- 1、指定專人辦理安全維護事項，防止本寺廟保有之個人資料被竊取、竄改、毀損、滅失或洩漏。
- 2、本寺廟保有之個人資料檔案，限承辦人員使用或存取，使用或存取範圍限與其本身業務相關，且存取檔案時須鍵入其個人之使用者代碼及識別密碼。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經負責人或經授權之管理人員同意。
- 3、存有個人資料之儲存媒體(含可攜式媒體)，視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。
- 4、存有個人資料之紙本及存放媒介物於報廢汰換或轉作其他

用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀。

5、電腦系統安裝防毒軟體並定期更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。

6、對內或對外從事個人資料傳輸時，加強管控避免外洩。

7、加強所屬人員教育宣導，並嚴加管制。

（二）通報及應變：

1、本寺廟所屬人員發現個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故時，即時向負責人通報；發生安全事故之個人資料達5,000筆者，自發現時起72小時內，以內政部訂頒之「個人資料事故通報及紀錄表」通報臺南市政府並副知內政部。

2、發生個人資料安全事故時，儘速以適當方式通知當事人事故發生之事實、已採取之處理措施以及本寺廟窗口電話等資訊。

3、發生個人資料安全事故後，針對事故發生原因研議改進措施。

五、個人資料蒐集、處理及利用之內部管理措施

（一）所屬人員直接向當事人蒐集個人資料時，明確告知當事人以下事項：

1、本寺廟名稱。

2、蒐集目的。

3、個人資料之類別。（註：可參考法務部「個人資料保護法之特定目的及個人資料之類別」<https://mojlaw.moj.gov-tw/LawContent.aspx?LSID=f1010631>。）

4、個人資料利用之期間、地區、對象及方式。

5、當事人得向本寺廟請求閱覽、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，以及如不提供對其權益之影響。

- (二) 所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應立即停止處理、利用其個人資料。
- (三) 另本寺廟保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。
- (四) 當事人得向本寺廟表示拒絕提供，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之聯絡窗口為負責人。以上聯絡資料公告於本寺廟處所。如拒絕當事人行使上述權利，應附理由通知當事人。
- (五) 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。
- (六) 本寺廟所屬人員輸出、輸入個人資料時，須鍵入其個人之使用者代碼及識別密碼，並須在使用範圍及使用權限內為之。識別密碼應保密，不得洩漏或與他人共用。
- (七) 本寺廟所屬成員退出團體或離職時，主動刪除或銷毀其個人資料，並留存相關紀錄。
- (八) 指定管理人員每____年清查本寺廟所保有之個人資料是否符合特定目的，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，並留存相關紀錄。
- (九) 本寺廟保有之個人資料如需作特定目的外利用，應先行檢視是否符合個人資料保護法第 20 條第 1 項但書之規定。
- (十) 本寺廟委託他人或其他宗教團體蒐集、處理或利用個人資料時，對受託者為適當之監督並與其明確約定相關監督事項。

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、指派專人管理儲存個人資料之電腦及其他儲存媒介物，每____年清點、保養維護、資料備份，並注意設備防竊、未經授權攜出等安全措施。

- 2、重要個人資料備份應異地存放，並建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。
- 3、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。
- 4、電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，檢視個人資料是否確實刪除。

（二）資料安全管理

1、資通訊系統存取個人資料之管控：

- （1）於儲存個人資料之電腦設置識別密碼、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關閉檔案，不得任其停留於螢幕上。
- （3）每____年進行防毒、掃毒等必要之安全措施。
- （4）重要個人資料檔案應另加設密碼，非經陳報負責人核可不得存取。
- （5）所屬人員非經本寺廟負責人核可，不得任意複製本寺廟保有之個人資料檔案。
- （6）本寺廟蒐集、處理或利用個人資料達1萬筆以上時，設置使用者身分確認及保護機制、個人資料顯示之隱碼機制（註：如將身分證字號末4碼以****標示）、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施，防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。

2、紙本資料之保管：

- （1）記載有個人資料之紙本文件，在未使用時存放於公文櫃內並上鎖。所屬人員非經負責人核可，不得任意複製、拍攝或影印。
- （2）丟棄記載有個人資料之紙本文件時，應先以碎紙設備進行處理。

（三）人員管理

1、依業務需求適度設定所屬人員（註：例如主管、非主管人員）對

個人資料蒐集、處理及利用之不同權限。

- 2、所屬人員登錄電腦之識別密碼，每_____個月變更1次。
- 3、所屬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。
- 4、本寺廟與所屬人員間之勞務、承攬及委任契約均列入保密條款及違約罰則，以促使其遵守個人資料保密義務（含契約終止後）。
- 5、所屬人員離職時，應即取消其登錄電腦之使用者代碼（帳號）及識別密碼。其在職期間所持有之個人資料應確實移交，不得私自複製、留存並在外繼續利用。
- 6、承辦相關業務之所屬成員每_____個月變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。

七、認知宣導及教育訓練

- （一）本寺廟每年不定期辦理或參與個人資料保護法實體或數位教育訓練，並留存相關紀錄或佐證資料。
- （二）對於新進人員給予特別指導，確保其明瞭個人資料保護相關法令規定及責任範圍。

八、個人資料安全維護稽核機制

- （一）本寺廟每年進行1次本計畫及處理方法執行情形之檢查，檢查結果向負責人提出報告，相關文件至少保存5年。
- （二）若檢查結果不合法令或有不合法令之虞，依下項事項規劃改善措施：
 - 1、確認不合法令之內容及發生原因。
 - 2、提出改善及預防措施方案。
 - 3、紀錄檢查情形及結果。

九、使用紀錄、軌跡資料及證據保存

- （一）本寺廟建置個人資料之電腦，其個人資料使用查詢紀錄，需每年備份並設定密碼，儲存該紀錄之儲存媒介物保存於適當處所以供備查。

- (二) 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，非經負責人核可，不得任意取出。
- (三) 以上使用紀錄、軌跡資料及相關證據至少留存5年。

十、個人資料安全維護之整體持續改善

本寺廟將隨時參酌業務及執行本計畫狀況、社會輿情、技術發展及相關法規定修等因素，檢討本計畫是否合宜，必要時予以修正，並於修正後15日內報主管機關臺南市政府。

十一、業務終止後之個人資料處理方法

本寺廟解散或經主管機關廢止登記後，所保有之個人資料依下列方式處理，不再繼續使用，並將相關紀錄報送主管機關臺南市政府：

- (一) 銷毀：銷毀之方法(註：如將紙本資料送焚化或以碎紙機絞碎，儲存於電腦磁碟及其他媒介物之資料，以消磁、折斷光碟片、擊毀硬碟等物理方式破壞等)、時間、地點及證明銷毀之方式(註：如執行銷毀之佐證照片或影片，標註日期、地點)。
- (二) 移轉：移轉之原因(註：如與其他團體合併、業務由其他團體辦理等)、對象、方法(註：如紙本移交，或以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片等儲存媒介物傳遞)、時間、地點及受移轉對象得保有該項個人資料之合法依據(註：依據個人資料保護法規定)。