內政部指定祭祀團體個人資料檔案安全維護管理辦法

條　　文	說　　明
第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。	本辦法訂定依據。
第二條　本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。	本辦法主管機關。
第三條　本辦法所稱祭祀團體，指取得派下全員證明書之祭祀公業、依法完成登記之祭祀公業法人、財團法人祭祀公業或社團法人祭祀公業。	本辦法祭祀團體之定義。
第四條　祭祀團體應訂定個人資料檔案安全維護計畫及解散後個人資料處理方法（以下簡稱本計畫及處理方法），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 祭祀團體依前項規定訂定本計畫及處理方法時，應視其規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十一條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之： 一、祭祀團體之組織規模及特性。 二、個人資料檔案之安全管理措施： （一）配置適當之人員及相當資源。 （二）界定蒐集、處理及利用個人資料之範圍。 （三）個人資料之風險評估及管理機制。 （四）事故之預防、通報及應變機制。 （五）個人資料蒐集、處理及利用之內部管理程序。 （六）設備安全管理、資料安全管理及人員管理措施。 （七）認知宣導及教育訓練。 （八）個人資料安全維護稽核機制。 （九）使用紀錄、軌跡資料及證據保存。	一、依個人資料保護法（以下簡稱本法）第二十七條第二項規定，於第一項指定祭祀團體應訂定個人資料檔案安全維護計畫及解散後個人資料處理方法（以下簡稱本計畫及處理方法）。 二、本辦法規定之相關組織及程序要求，祭祀團體應明定於本計畫及處理方法內，並定期檢視及配合相關法令修正。 三、參照本法施行細則第十二條第二項規定意旨，所採行之安全措施與所欲達成之個人資料保護目的間，具有適當比例為原則。爰第二項規定祭祀團體得參考其規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十一條及本法施行細則第十二條第二項規定，訂定適宜並符合比例原則之安全措施，據以執行。另保留彈性空間，得依個別情況於必要時整併第二款各目之相關事項。 四、第三項定明祭祀團體訂定本計畫及處理方法報請主管機關備查之期限。

（十）個人資料安全維護之整體持續改善。 （十一）解散後之個人資料處理方法。 第一項之本計畫及處理方法，祭祀團體應於取得派下全員證明書或法人登記證書之日起六個月內報請祭祀團體或主事務所所在地之直轄市、縣（市）主管機關備查。	
第五條　祭祀團體應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並定期向管理人提出報告。 祭祀團體應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於主事務所或祭祀場所適當之處；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。	一、第一項規定祭祀團體應指派配置適當管理人員，負責本計畫及處理方法之規劃、訂定、修正及執行等事宜，並提供適當之資源協助，以為確保個人資料維護安全措施發揮效能。另本法第四十八條第四款及第五十條規定，對違反本法第二十七條第一項或未依同條第二項訂定本計畫及處理方法之祭祀團體之代表人、管理人或其他有代表權人得併同處罰。爰規定負責本計畫及處理方法之人員須定期向管理人提出報告，促使管理人能據以監督本計畫及處理方法之執行，落實對個人資料保護之工作。所稱管理人，包含祭祀公業、祭祀公業法人之管理人、代表人及財（社）團法人祭祀公業之董（理）事長。 二、為能讓祭祀團體所屬人員明瞭個人資料保護之重要性，第二項規定祭祀團體應將個人資料保護管理政策及蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護，公告於主事務所或祭祀場所適當之處，以供所屬人員遵循，更可使當事人知曉祭祀團體保護個人資料之相關事項，俾保護自身權益。
第六條　祭祀團體應依個人資料保護相關法令，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。	祭祀團體蒐集個人資料應定期清查所蒐集保有之個人資料是否符合本計畫及處理方法所界定之範圍。
第七條　祭祀團體應依前條界定之個人資料範圍及其蒐集、處理及利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂	定明祭祀團體應參考整體業務運作狀況，就已界定個人資料之範圍與蒐集、處理及利用個人資料流程，分析評估可能發生之風險，並針對該可能發生之風

定適當之管控機制。	險，採取必要之防範與管控措施，避免個人資料被竊取、竄改、毀損、滅失、洩漏或濫用。
第八條　祭祀團體為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應訂定下列應變、通報及預防機制： 一、個人資料事故發生後應採取之各類措施，包括： （一）控制當事人損害之方式。 （二）查明個人資料事故後通知當事人之適當方式。 （三）應通知當事人個人資料事故事實、所為因應措施及諮詢服務專線等內容。 二、個人資料事故發生後應受通報之對象及其通報方式。 三、個人資料事故發生後，其矯正預防措施之研議機制。 祭祀團體遇有達五百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，以書面通報祭祀團體或主事務所所在地直轄市、縣（市）主管機關，並副知中央主管機關（書面通報格式如附件）。 直轄市、縣（市）主管機關對於重大個人資料事故，得依本法第二十二條規定對祭祀團體之應變、通報及預防機制進行實地檢查，並視檢查結果為後續處置。中央主管機關認有必要時，得督導直轄市、縣（市）主管機關對於祭祀團體之相關機制改善情形。	一、本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查明後以適當方式通知當事人。爰第一項定明祭祀團體在本計畫及處理方法中應訂定應變機制及其必要作為之相關事項，在發生個人資料被竊取等侵害事故時，得迅速遵循處理，以保護當事人之權益。 二、第二項考量多數祭祀團體為千人以下之規模，爰定明祭祀團體遇有達五百筆以上之個人資料被竊取、洩漏、竄改或其他侵害之重大個人資料事故時，負通報義務。並依行政院一百十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，定明事故通報時點及應通報事項。 三、為調查事故發生後，是否係祭祀團體所採取保護安全措施不足導致，第三項定明中央及直轄市、縣（市）主管機關對於重大個人資料事故得採取之措施及後續行政檢查規定。
第九條　祭祀團體所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第	定明祭祀團體所屬人員執行業務蒐集、處理及利用一般個人資料時，應遵守相關法定要件及程序。

一項但書情形。	
第十條　祭祀團體蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。	為尊重當事人能知曉其個人資料被蒐集、處理及利用之狀況，本法第八條及第九條規定資料蒐集者有告知義務。爰規定祭祀團體，應區分個人資料蒐集方式為直接蒐集或間接蒐集，分別訂定告知之方法、內容及相關注意事項，以便所屬人員在辦理業務時能據以執行。
第十一條　中央主管機關依本法第二十一條規定，對祭祀團體為限制國際傳輸個人資料之命令或處分時，祭祀團體應通知所屬人員遵循辦理。 祭祀團體將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督： 一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。 二、當事人行使本法第三條所定權利之相關事項。	一、第一項規定中央主管機關依本法第二十一條規定所為之命令或處分，祭祀團體應通知所屬人員知曉並遵照辦理。 二、第二項規定祭祀團體將個人資料作國際傳輸者，應檢視是否受中央主管機關依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督。
第十二條　祭祀團體於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理： 一、提供聯絡窗口及聯絡方式。 二、確認為個人資料當事人本人，或經其委託者。 三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。 四、有收取必要成本費用者，應告知當事人收費基準。 五、遵守本法第十三條有關處理期限規定。	依本法第三條規定，當事人就其個人資料得行使查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除其個人資料等權利，且祭祀團體除有本法第十條但書、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之情形外，應於本法第十三條規定期間內准駁當事人之請求，爰定明祭祀團體應辦理事項，以利資料當事人行使權利。
第十三條　祭祀團體對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。 前項安全設備或防護措施，應包含下列事項： 一、紙本資料檔案之安全保護設施。 二、電子資料檔案存放之電腦、自	為確保祭祀團體所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰第一項規定祭祀團體得視其規模、業務性質、資料儲存之媒介物及其數量等，於所定本計畫及處理方法中採取必要且適當之安全設備或防護措施。第二項並規定安全設備或防護措施應包括事

動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。 三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，祭祀團體對受託者之監督依第二十條規定辦理。	項，例如：對紙本資料之保護應採用堅固之保險箱或櫥櫃；電腦設備應設置防火牆及防毒程式、對複製或上傳檔案行為予以管控、制定紙本資料之銷毀程序、磁碟、磁帶、光碟片、微縮片、積體電路晶片及其他存放個人資料之媒介物需報廢汰換或轉作其他用途時，應確實刪除所存放之個人資料檔案或防範洩漏個人資料等。
第十四條　祭祀團體為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。 前項管理措施，應包含下列事項： 一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。 三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。 四、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。	一、祭祀團體與所屬人員，不論是何種法律關係，祭祀團體都必須避免個人資料之保管及處理發生弊端，導致侵害當事人權益情事，爰第一項規定應於所定本計畫及處理方法中，對所屬人員採取必要且適當之管理措施。 二、第二項規定祭祀團體應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：與業務無關人員不得任意接觸資料、授予必要利用個人資料人員不同等級之權限、所屬人員在個人資料蒐集、處理及利用流程中有無漏洞、約束規範嚴密保管個人資料檔案及所屬人員異動或離職時，所持有之個人資料如何交接與保密切結等事項。
第十五條　祭祀團體使用資通訊系統蒐集、處理或利用個人資料達三千筆以上者，應採取下列資訊安全措施： 一、使用者身分確認及保護機制。 二、個人資料顯示之隱碼機制。 三、網際網路傳輸之安全加密機制。 四、個人資料檔案與資料庫之存取控制及保護監控措施。 五、防止外部網路入侵對策。 六、非法或異常使用行為之監控及因應機制。 前項第五款及第六款所定措施，應定期演練及檢討改善。	一、依據行政院一百十年二月三日會議決議事項，非公務機關使用資通訊系統蒐集、處理或利用個人資料，為避免使用者個人資料於使用資通訊服務時被竊取、洩漏、竄改或其他侵害事故發生，並參照行政院資通安全處建議採取之資訊安全措施，於第一項定明祭祀團體使用資通訊系統保有個人資料筆數達三千筆以上者，應訂定之資訊安全措施，以落實保護個人資料。另參考資通安全責任等級分級辦法附表十資通系統防護基準，針對六項資訊安全措施之實作說明如下：

	（一）系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。 （二）系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考CNS二九一九一「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準。 （三）個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。 （四）儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。 （五）針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。 （六）針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。 二、祭祀公業之性質為具一定親屬關係之團體，其成員以具派下員身分為限，查現行祭祀團體多數為千人以下之規模，考量派下員之繼承方式及個人資料累積規模，爰第一項訂定祭祀團體使用資通訊系統保有個人資料筆數達三千筆以上者，應採取資訊安全措施。 三、隨網路科技之進步，個人資料遭外部網路入侵或非法或異常使用行為

	損害情形層出不窮，爰第二項定明針對第一項第五款及第六款所定措施，祭祀團體應定期進行演練及檢討改善。
第十六條　祭祀團體應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。	定明祭祀團體應定期或不定期對所屬人員施以認知宣導或教育訓練，以使所屬人員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。
第十七條　祭祀團體為確保本計畫及處理方法之落實，應依其組織規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次本計畫及處理方法執行情形之檢查。 前項檢查結果應向管理人提出報告，並留存相關紀錄，其保存期限至少五年。 祭祀團體依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。	一、第一項及第二項規定祭祀團體訂定之本計畫及處理方法應包含安全稽核機制，由適當人員檢查該本計畫及處理方法是否落實執行，並應將檢查結果報告祭祀團體管理人，並須留存相關紀錄至少五年。 二、第三項規定檢查結果發現本計畫及處理方法不符法令者，祭祀團體應作必要之改善。
第十八條　祭祀團體執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。 祭祀團體依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。	第一項定明祭祀團體應記錄其個人資料使用情況，並留存軌跡資料或相關證據；另於第二項規定依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料時，亦應留存相關紀錄；且於第三項規範上述軌跡資料、相關證據及紀錄，除法令另有規定或契約另有約定者外，應至少留存五年。
第十九條　祭祀團體應隨時參考業務及本計畫及處理方法執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必	由於科技發展不斷進步，社會活動型態亦隨時改變，爰定明祭祀團體應注意媒體對個人資料侵害或保護事件相關報導，並配合個人資料保護法令之訂修，

要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請祭祀團體或主事務所所在地之直轄市、縣（市）主管機關備查。	隨時檢討所定本計畫及處理方法，如有不合時宜之處，應立即修正本計畫及處理方法，以落實保護個人資料。
第二十條　祭祀團體委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。 祭祀團體為執行前項監督，應與受託者明確約定相關監督事項及方式。	依本法施行細則第八條之規定，委託他人蒐集、處理或利用個人資料時，委託者應為適當之監督，避免受託者有違反本法情事發生，爰第一項定明祭祀團體委託他人蒐集、處理或利用個人資料之全部或一部時，應為適當之監督，並於第二項規定與受託者約定相關監督事項及方式。
第二十一條　祭祀團體因解散或經主管機關廢止登記後，其保有之個人資料不得繼續使用，應依下列方式處理，並將相關紀錄報送祭祀團體或主事務所所在地直轄市、縣（市）主管機關保存至少五年： 一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。 二、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。 三、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。	一、祭祀團體解散或經主管機關廢止登記後，自不得再繼續持有使用個人資料，應作妥善處置。爰規定祭祀團體，應將所保有之個人資料予以銷毀、移轉或其他刪除、停止處理或利用等方式處理，並將相關紀錄報送主管機關保存一定期間。 二、祭祀團體在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，宜保存執行方法、時間、地點、執行人員、接受移轉個人資料之對象及合法移轉個人資料之法規依據等資料，以便日後舉證。
第二十二條　本辦法發布施行前，未訂定本計畫及處理方法之祭祀團體，應依本辦法規定訂定，並於本辦法發布施行日起六個月內，將本計畫及處理方法報請祭祀團體或主事務所所在地之直轄市、縣（市）主管機關備查。	規範本辦法施行前之祭祀團體，應依本辦法訂定本計畫及處理方法，並於一定期間內報備查。
第二十三條　本辦法自發布日施行。	本辦法施行日期。

附件

<table>
<tr><td colspan="3">個人資料事故通報及紀錄表</td></tr>
<tr><td>祭祀團體名稱
_____
通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名（蓋章）
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個人資料____筆
□特種個人資料____筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□是　□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。

說明：

依據第八條第二項規定，定明祭祀團體遇個人資料侵害事故發生後，應依本表格式通報直轄市、縣（市）主管機關，並副知中央主管機關。