（社會福利財團法人名稱）個人資料檔案安全維護計畫（範本格式）

○○○年○○月○○日第○屆第○次董事會議通過訂定
○○○年○○月○○日第○屆第○次董事會議通過修訂

＊範本格式僅供參考，請依個人資料保護相關法規、內部管理作業程序及實際業務情形，訂定個人資料檔案安全維護計畫，及業務終止後個人資料處理方法等相關事項。

壹、依據及目的

一、依據個人資料保護法（以下稱本法）第27條第3項及社會福利財團法人個人資料檔案安全維護計畫實施辦法第4條，社會福利財團法人（以下稱社福法人）應訂定個人資料檔案安全維護計畫（以下稱本計畫）。

二、落實社福法人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。

貳、組織規模

一、主事務所地址：○○○（捐助章程及法人登記證書上之地址）

二、分事務所地址：○○○（如果多個分事務所，請分別列示地址）

三、實際辦公地址：○○○（如有多處辦公地點，請分別列示地址）

四、所屬人員人數：約○○人（包括管理組織人員、職員、志工等）

參、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）專責人員

1、配置人數：○人。（至少配置1名）

2、職責：負責規劃、訂定、修正及執行本計畫，及業務終止後個人資料處理方法與其他相關事項，並每○○日（或週、月、季、年）向○○○（董事長或管理組織名稱）提出報告。

（二）查核人員

1、配置人數：○人。（至少配置1名，且不得與專責人員為同一人）

2、職責：負責定期每○○日（或週、月、季、年）稽核本計畫之執行情形及成效之人員，並出具稽核報告，必要時向○○○

（董事長或管理組織名稱）提出改善計畫。

（三）經費預算：每年約新臺幣○○元。（包含管理薪資、設備維護費用等；可記載一定範圍之金額，請依實際狀況填寫）

二、個人資料蒐集、處理及利用之內部管理程序

（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、本社福法人名稱。

2、蒐集之目的。

3、個人資料之類別。（可參考個人資料保護委員會籌備處「個人資料保護法之特定目的及個人資料之類別」https://theme.ndc.gov.tw/lawout/LawContent.aspx?id=GL000316）

4、個人資料利用之期間、地區、對象及方式。

5、當事人得向本社福法人請求閱覽、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，不提供對其權益之影響。

（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；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）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19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20條第1項但書情形。

（四）當事人得向本社福法人表示拒絕提供，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，其聯絡窗口為○○○；聯絡電話：○○○○○。以上聯絡資料公告於本社福法人處所（有網站或其他適當處所者，請增列網站首頁及其他適當地點，如分事務所、附屬作業組織名稱）。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，應移交所保管於儲存媒體之有關資料檔案。

（六）所屬人員如因其工作職掌相關而需輸出、輸入個人資料時，均需鍵入其個人之使用者代碼及識別密碼，且在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與其他人共用。

（七）由管理組織或經指定之人員（專責人員或所屬人員）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，除因法令規定、執行業務所必須或經當事人同意者，應即予刪除、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。

（八）所屬人員於國際傳輸個人資料前，應檢視未受主管機關限制，及無本法第21條4種例外情形（①涉及國家重大利益；②國際條約或協定有特別規定；③接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞；④以迂迴方法向第三國(地區)傳輸個人資料規避本法），始得合法進行國際傳輸，並應告知當事人擬傳輸之國家或區域，同時對資料接收方為下列事項之監督：

1、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。

2、當事人行使本法第3條所定權利之相關事項。

（九）本社福法人委託他人蒐集、處理或利用個人資料時，應對受託方為適當之監督，並與其明確約定相關監督事項。

（十）○○○。(依實際情形自行增列)

三、個人資料之範圍及項目

（一）個人資料範圍

指本社福法人蒐集、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。（可參考本法第2條第1款填寫）

（二）蒐集、處理及利用個人資料之特定目的：（可參考個人資料保護委員會籌備處「個人資料保護法之特定目的及個人資料之類別」，若查無相對應之特定目的及類別，得自由敘述補充）

1、人事管理。

2、非營利組織業務。

3、本社福法人對董事、監察人及所屬人員名冊之內部管理。

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。（例如：疫情期間實名制相關資料）

6、○○○。（依實際情形自行增列）

四、資料安全管理及人員管理

（一）資料安全管理

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、每○○日（或週、月、季、年）進行電腦系統防毒、掃毒等必要之安全措施。

4、重要個人資料應另加設管控密碼，並每○○日（或週、月、季、年）更換密碼，非經陳報○○○（請填董事長、管理組織或指定之人員(專責人員或所屬人員)，依實際情形填寫）核可，不得存取。

5、所屬人員非經本社福法人○○○（請填董事長、管理組織或指定之人員(專責人員或所屬人員)，依實際情形填寫）核可，並取得密碼者，不得存取本社福法人保有之個人資料檔案。

6、本社福法人蒐集、處理或利用個人資料達○筆以上時，應設置

使用者身分確認及保護機制、個人資料顯示之隱碼機制（例如：將身分證字號末4碼以****標示，或將姓名其中1個字以○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。

7、○○○。（依實際情形自行增列）

（二）人員管理

1、本社福法人應依業務需求設定所屬人員（例如主管、非主管人員）不同之權限，以控管其個人資料蒐集、處理與利用之情形。

2、本社福法人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、本社福法人所屬人員應妥善保管個人資料之儲存媒介物；執行業務時應依本法規定蒐集、處理及利用個人資料。

4、本社福法人所屬人員離職，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（如在職時之相關勞務契約已有所約定時，亦屬之）。

5、本社福法人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）。

6、本社福法人所屬人員每○○日（或週、月、季）變更識別密碼一次，並於變更識別密碼後始可繼續使用電腦。

7、○○○。（依實際情形自行增列）

五、事故之預防、通報及應變機制

（一）預防

1、本社福法人所屬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、本社福法人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，應經董事長、管理組織或經指定之人員（專責人員或所屬人員）同意。

3、個人資料於本社福法人與所屬單位（分事務所）、附屬作業組織、機構間或相關單位互為傳輸時，應加強管控避免外洩。

4、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。

5、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。

6、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。

7、對內或對外從事個人資料傳輸時，加強管控避免外洩。

8、加強員工教育宣導，並嚴加管制。

9、○○○。（依實際情形自行增列）

（二）通報及應變

1、**【適用全國性社福法人】**本社福法人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○○○（董事長或管理組織名稱）通報；發生個人資料安全事故時，自發現時起72小時內，以衛生福利部訂頒之「個人資料侵害事故通報紀錄」通報衛生福利部。

【適用地方性社福法人】本社福法人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○○○（董事長或管理組織名稱）通報；發生個人資料安全事故時，自發現時起72小時內，以衛生福利部訂頒之「個人資料侵害事故通報紀錄」通報直轄市或縣（市）政府（例如：基隆市、臺

北市、臺東縣）並副知衛生福利部。

2、發生個人資料安全事故時，儘速以適當方式通知當事人個人資料受侵害之事實、已採取之因應措施，及本社福法人連繫窗口電話等資訊。

3、發生個人資料安全事故後，針對該事故研議精進措施，避免類似事故再次發生。

4、○○○。（依實際情形自行增列）

六、設備安全管理

（一）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。

（二）指派專人管理儲存個人資料之電腦及其他儲存媒介物，每○○日（或週、月、季、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。

（三）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。

（四）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。

（五）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，亦檢視個人資料是否確實刪除。

（六）對於各類契約書件及記載有個人資料之紙本文件，應存放於公文櫃內並上鎖，員工非經董事長、管理組織或經指定之人員（專責人員或所屬人員）同意，不得任意複製、拍攝或影印。

（七）丟棄記載個人資料之紙本時，應先碎紙設備進行處理。

（八）○○○。（依實際情形自行增列）

七、資料安全稽核機制

（一）本社福法人定期（每半年至少一次，每年○次）辦理個人資料安全維護稽核，檢查是否落實本計畫規範事項，針對檢查結果不符合法令及潛在不符合之風險，應即改善，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、確認不符合法令之內容及發生原因。

2、提出改善及預防措施方案。

3、記錄檢查情形及結果。

（二）前項檢查結果應載入稽核報告中，由○○○（董事長、管理組織或經指定之人員(專責人員或所屬人員)）簽名確認，並留存相關紀錄至少保存5年。

（三）○○○。(可依實際情形自行增列)

八、使用紀錄、軌跡資料及證據保存（本項請視社福法人規模及業務性質，採行適當措施，依實際情形說明如何保存個人資料相關使用紀錄及自動化機器設備之軌跡資料）

（一）本社福法人建置個人資料之電腦，其個人資料使用查詢紀錄檔，需每○月（或季、年）備份並設定密碼（加密），並將該紀錄檔之儲存媒介物保存於適當處所以供備查。

（二）採紙本登記之個人資料使用紀錄，應存放於公文櫃內並上鎖，非經○○○（董事長、管理組織或經指定之人員(專責人員或所屬人員)）同意，不得任意取出及查閱。

（三）○○○。(依實際情形自行增列)

（四）以上使用紀錄、軌跡資料及相關證據，應至少留存5年。

九、業務終止後之個人資料處理方法

針對個人資料之銷毀、移轉或刪除、停止處理或利用等作業，應依下列規範處理，並留存相關紀錄；紀錄至少留存5年。(本項請依實際情形敘明)

（一）銷毀：執行之人員、方法、時間、地點及證明銷毀之方式。

□書面個人資料已送焚化或以碎紙機絞碎；儲存於電腦磁碟及其他媒介物之個人資料已消磁、折斷光碟片、擊毀硬碟等物理方式破壞其功能。

□其他：(請依實際情形填寫)

以上行為請拍照存證（照片需印日期並揭露地點）或錄影存證（影片需有日期並揭露地點）。

（二）移轉：執行之人員、原因（如與其他財團法人合併、業務由其他單位辦理等）、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。

移轉之原因：□業務需要

□其他：（請依實際情形填寫）

移轉之對象：（請依實際情形填寫）

移轉之方法：□紙本移交傳遞。

□以電腦磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他存放媒介物等傳遞。

□其他：（請依實際情形填寫）

受移轉對象得保有該項個人資料之合法依據：○○○。

（三）刪除、停止處理或利用：執行之人員、方法、時間或地點。（請依實際情形填寫）

十、個人資料安全維護之整體持續改善方案

（一）**【適用全國性社福法人】**本社福法人隨時依計畫執行狀況、社會輿情、技術發展、法令修正或其他因素，檢視本計畫之合宜性，必要時予以修正，並於修正後15日內報主管機關衛生福利部備查。

【適用地方性社福法人】本社福法人隨時依計畫執行狀況、社會輿情、技術發展、法令修正或其他因素，檢視本計畫之合宜性，必要時予以修正，並於修正後15日內報主管機關直轄市或縣（市）政府（例如：基隆市、臺北市、臺東縣）備查。

（二）本社福法人每年（或○月）辦理個人資料保護認知宣導及教育訓練至少○次（或每年指派○人參與相關單位辦理之教育訓練（含數位學習）至少○小時，請依實際情況填寫），使員工知悉並

遵守相關規定；上述教育宣導及訓練應留存紀錄（如：簽到表或照片等佐證資料）。

（三）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、責任範圍及應遵守之相關管理措施。

（四）○○○。（依實際情形自行增列）