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 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。

第 二 條　　本辦法所稱主管機關：在中央為衛生福利部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第 三 條　　本辦法用詞，定義如下：

一、社會福利財團法人（以下簡稱社福法人）：指屬主管機關依財團法人法第二十四條第三項所定財產總額或年度收入總額達一定金額以上之財團法人。

二、專責人員：指由社福法人指定，負責個人資料檔案安全維護計畫（以下簡稱安全維護計畫）訂定及執行之人員。

三、所屬人員：指社福法人執行業務過程中接觸個人資料之人員。

四、查核人員：指由社福法人指定，負責稽核安全維護計畫執行情形及成效之人員。

前項第一款社福法人為社會福利機構個人資料檔案安全維護計畫實施辦法所定社會福利機構者，其個人資料檔案之管理，依該辦法之規定為之，不適用本辦法之規定。

第一項第二款專責人員與第四款查核人員，不得為同一人。

第 四 條　　社福法人應依本辦法規定，訂定安全維護計畫，並報主管

機關備查。

前項安全維護計畫，應載明下列事項：

一、個人資料蒐集、處理及利用之內部管理程序。

二、個人資料之範圍及項目。

三、資料安全管理及人員管理。

四、事故之預防、通報及應變機制。

五、設備安全管理。

六、資料安全稽核機制。

七、使用紀錄、軌跡資料及證據保存。

八、業務終止後個人資料處理方法。

九、個人資料安全維護之整體持續改善方案。

第 五 條　　社福法人執行業務，以本法第六條所定個人資料種類之資通系統，蒐集、處理或利用其當事人之個人資料，除依前條規定辦理外，並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、應用系統於開發、上線、維護及其他階段軟體驗證與確認程序。

五、個人資料檔案及資料庫存取控制與保護監控措施。

六、防止外部網路入侵對策。

七、非法或異常使用行為之監控及因應機制。

前項所稱資通系統，指用以蒐集、控制、傳輸、儲存、流

通、刪除資訊或對資訊為其他處理、使用或分享之系統。

第一項第六款、第七款所定措施，社福法人應定期演練及檢討改善。

第 六 條　社福法人應依其業務規模及特性，衡酌經營資源之合理分配，規劃、訂定、檢討、修正安全維護措施，納入安全維護計畫，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。

第 七 條　專責人員應負責規劃、訂定、修正、執行安全維護計畫，及業務終止後個人資料處理方法與其他相關事項，並定期向社福法人提出報告。

第 八 條　社福法人訂定第四條第二項第一款個人資料蒐集、處理及利用之內部管理程序、第二款個人資料之範圍及項目，應包括下列事項：

一、個人資料之蒐集、處理，應符合本法第十九條規定。

二、個人資料之利用，應符合本法第二十條規定。

三、定期檢視保有之個人資料，發現有非屬特定目的範圍內之個人資料、特定目的消失、期限屆至而無執行職務或業務所必須或經當事人同意者，應予刪除、銷毀、停止蒐集、處理、利用或為其他適當之處置。

四、個人資料之傳輸，應採取必要保護措施，避免洩漏。

五、個人資料之蒐集，應依本法第八條第一項及第九條第一項規定，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。

第 九 條　　社福法人訂定第四條第二項第三款資料安全管理及人員管理，應包括下列事項：

一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之必要性及適當性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理、利用及其他相關流程之負責人員。

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、所屬人員離職時，取消其識別碼，並令其將執行業務所持有之紙本及儲存媒介物之個人資料辦理交接，不得攜離使用，及簽訂保密切結書。

第 十 條　　社福法人訂定第四條第二項第四款事故之預防、通報及應變機制，應包括下列事項：

一、採取適當之措施，控制事故對當事人造成之損害。

二、查明事故發生原因及損害狀況，以適當方式通知當事人或其法定代理人。

三、研議改進措施，避免事故再度發生。

四、社福法人發生事故者，應於發現時起七十二小時內，通報主管機關；主管機關得依本法第二十二條至第二十五條規定，為適當之監督管理措施。其屬直轄市、縣（市）主管機關主管者，於通報時，並應副知中央主管機關。

社福法人於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事故時，應依前項事項之預防、通報及應變機制迅速處理，保護當事人之權益。

第一項第四款通報紀錄，格式如附表。

第十一條　社福法人訂定第四條第二項第五款設備安全管理，應包括下列事項：

一、紙本資料檔案之安全保護設施及管理程序。

二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

三、紙本及電子資料之銷毀程序。

四、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，應採取適當防範措施，避免洩漏個人資料。

第十二條　查核人員應依第四條第二項第六款規定，定期或不定期稽核安全維護計畫之執行情形及成效，並出具稽核報告，必要時向社福法人提出改善計畫。

第十三條　社福法人訂定第四條第二項第七款使用紀錄、軌跡資料及證據保存，應包括下列事項：

一、留存個人資料使用紀錄。

二、留存自動化機器設備之軌跡資料或其他相關之證據資料。

三、前二款紀錄及資料證據之保存措施。

第十四條　社福法人訂定第四條第二項第八款業務終止後個人資料

處理方法，應包括下列事項：

一、銷毀：方法、時間、地點及證明銷毀之方式。

二、移轉：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、刪除、停止處理或利用：方法、時間或地點。

前項措施應製作紀錄，並至少留存五年。

第十五條　社福法人訂定第四條第二項第九款個人資料安全維護之整體持續改善方案，應參酌安全維護計畫執行狀況、技術發展、法令修正或其他因素，檢視所定安全維護計畫之合宜性，必要時應予修正。

第十六條　社福法人將當事人個人資料為國際傳輸前，應檢視有無受中央主管機關依本法第二十一條規定為國際傳輸之限制，並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：

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。

第十七條　社福法人應於本辦法發布施行後一年內，完成安全維護計畫之訂定及實施；主管機關得定期派員檢查。

第十八條　本辦法自發布日施行。

附表

<table>
<tr><td colspan="2">個人資料侵害事故通報紀錄表</td></tr>
<tr><td>社福法人名稱：</td><td rowspan="2">首次通報時間：　年　月　日　時　分
通報人：　　簽名（蓋章）
職稱：
電話：
電子信箱：
地址：</td></tr>
<tr><td>通報機關：</td></tr>
<tr><td>事件發生時間</td><td>年　　月　　日　　時　　分</td></tr>
<tr><td>事件發生種類</td><td>□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td></tr>
<tr><td>發生原因及事件摘要</td><td></td></tr>
<tr><td>損害狀況</td><td>個人資料侵害之總筆數（大約）_____筆
□一般個人資料_____筆
□特種個人資料_____筆
是否造成個人資料當事人財產損害：
□是，財損金額_____
□否
□其他損害情形，說明：_____</td></tr>
<tr><td>侵害可能結果</td><td></td></tr>
<tr><td>擬採取之因應措施</td><td></td></tr>
</table>

依本法第十二條及本法施行細則第二十二條，擬通知當事人之時間及方式	
是否於發現個人資料侵害事故時起七十二小時內通報	□是　□否，說明：

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。