社會福利機構個人資料檔案安全維護計畫實施辦法

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。	依個人資料保護法(以下簡稱本法)第二十七條規定:「(第一項)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項) 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。(第三項) 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」爰明定本辦法之法源依據。
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。	本辦法之主管機關。
第三條　本辦法用詞，定義如下： 一、社會福利機構，指下列機構： （一）依私立兒童及少年福利機構設立許可及管理辦法之規定，核定之床數逾九十五床之機構。 （二）依私立老人福利機構設立許可及管理辦法之規定，核定之床數逾二百床之機構。 （三）依私立身心障礙福利機構設立許可及管理辦法之規定，核定之床數逾二百床之機構。 二、專責人員:指由社會福利機構指定,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：指社會福利機構執行業務過程中接觸個人資料之人員。 四、查核人員:指由社會福利機構指定,負責稽核安全維護計畫執行情形及成效之人員。 前項第二款專責人員與第四款查核人員，不得為同一人。	一、社會福利機構之樣態多元，包含公私立機構、法人或團體，審酌社會福利機構規模、特性、保有個人資料之性質及數量，以及社會福利機構類型及執行可行性，並考量多數私立兒童及少年福利機構核定床數皆未達一百床，為使實施範疇具一致性，本辦法適用對象僅限於核定床數逾九十五床之私立兒童及少年福利機構；核定床數逾二百床之私立老人福利機構、私立身心障礙福利機構之私立社會福利機構。 二、公立社會福利機構係屬個人資料保護法之公務機關，不適用本辦法之規定。 三、為使安全維護計畫有效運作，爰於第一項明定個人資料安全維護相關人員，包括專責人員、所屬人員及查核人員，並規定所有人員之定義。

	四、為確保查核制度獨立及確實執行，爰於第二項明定專責人員與查核人員不得為同一人。
第四條　社會福利機構應依本辦法規定，訂定安全維護計畫，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。	考量社會福利機構規模不一，經營主體與型態未盡相同，尚難作統一規範，爰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，訂定安全維護計畫項目如條文所示內容，使其符合社會福利機構特性之比例原則。
第五條　社會福利機構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。	適用本辦法之社會福利機構應配置相當資源，俾規劃、訂定、檢討、修正與執行安全維護計畫之相關事項，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。
第六條　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，並定期出具報告及提出改善計畫。	依本法施行細則第十二條規定，本法第二十七條第一項所稱適當之安全措施，指為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括配置管理之人員及相當資源，為有效訂定與執行本計畫，社會福利機構應指定專人辦理有關事項，爰明定專責人員之任務。
第七條　社會福利機構訂定第四條第一款、第二款規定時，應確認蒐集個人資料之特定目的及其必要性，界定所蒐集、處理及利用個人資料之類別及範圍，並定期清查所保有之個人資料現況。 社會福利機構經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆至無保存必要者，應予刪除、銷毀、	一、社會福利機構應依本法施行細則第十二條第二項第二款之規定，於安全維護計畫中就界定個人資料範圍相關事項加以規定，爰於第一項明定社會福利機構應依蒐集之特定目的，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查其現況。

停止蒐集、處理、利用或為其他適當之處置。	二、為維護當事人權益，爰於第二項明定社會福利機構對個人資料應定期檢視及清查，並為適當處置。
第八條　社會福利機構蒐集個人資料時，應符合前條第一項所定之類別及範圍。 社會福利機構於傳輸個人資料時，應採取必要保護措施，避免洩漏。	一、第一項明定社會福利機構蒐集個人資料，應符合前條第一項所定之類別及範圍。 二、第二項明定社會福利機構如有傳輸個人資料之情事，應採取必要保護措施，避免洩漏。
第九條　社會福利機構蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並依直接或間接蒐集，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。	一、社會福利機構依本法第八條及第九條規定，如有例外免告知事由者，並應確認該事由是否符合規定。 二、社會福利機構應採取適當告知方式以履行告知義務。
第十條　社會福利機構將當事人個人資料為國際傳輸前，應檢視是否受中央主管機關限制，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。	社會福利機構將個人資料為國際傳輸前，應履行告知義務之規定，同時對資料接收方為相關事項監督。
第十一條　社會福利機構訂定第四條第三款資料安全管理及人員管理之措施，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，並要求將執行業務所持有，包括紙本及儲存媒介物	社會福利機構及其所屬人員，不論是何種法律關係，機構都應避免其保管、蒐集、處理及利用個人資料時，違反個人資料保護相關法令規定，導致侵害當事人權益情事，爰明定應採取必要且適當之管理措施。

之個人資料辦理交接，不得攜離使用，並簽訂保密切結書。	
第十二條　社會福利機構訂定第四條第四款事故之預防、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，並於發現事故時起七十二小時內，通報直轄市、縣（市）主管機關及通知中央主管機關。 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。 社會福利機構於發生個人資料被竊取、洩漏、竄改或其他侵害事故時，應依前項事故之預防、通報及應變機制迅速處理，保護當事人之權益。 社會福利機構發生前項事故者，主管機關得依本法第二十二條第一項規定進入檢查、命相關人員為必要之說明、配合措施或提供相關證明資料，並視檢查結果為後續處置。 第一項第一款通報紀錄格式如附表。	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或其法定代理人，爰於第一項明定社會福利機構在安全維護計畫中應訂定應變機制及執行事項。 二、第二項明定社會福利機構於個人資料被竊取等侵害事故時，應依前項事故之預防、通報及應變機制迅速處理，保護當事人之權益。 三、第三項明定社會福利機構發生個人資料侵害事故，主管機關得依本法第二十二條規定辦理檢查，並視檢查結果為後續處置之規定。 四、第四項明定個人資料侵害事故通報紀錄表格式。
第十三條　社會福利機構訂定第四條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，應採取適當防護措施，避免洩漏個人資料。	為確保社會福利機構所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，業者得視其規模、業務性質、資料儲存媒介物及其數量等，爰明定社會福利機構對所保有之個人資料，應設置必要之安全設備管理及採取必要之防護措施，避免洩漏個人資料。
第十四條　查核人員應依第四條第六款規定，定期或不定期稽核安全維護計畫之執行情形，並出具稽核報告，必要時向社會福利機構提出改善計畫。	為確保個人資料維護安全措施發生效能，明定社會福利機構應訂定個人資料檔案安全維護稽核機制，定期或不定期檢查安全維護計畫之執行情形。依本法第五十條規定，對非公務機關之代表人，

	因該非公務機關依本法第四十七條至第四十九條規定受罰鍰處罰時，除能證明已盡防止義務者外，應受同一額度罰鍰，爰規定向社會福利機構提出檢查結果報告，促使社會福利機構得據以監督安全維護計畫之執行事項，落實對個人資料保護之工作。
第十五條　社會福利機構訂定第四條第七款使用紀錄、軌跡資料及證據保存之措施，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。	社會福利機構為證明確實執行安全維護計畫，已盡防止個人資料遭侵害之義務，應視其規模及業務性質採行適當措施，留存相關證據，以供日後發生問題時提供說明佐證，以釐清其法律責任。
第十六條　社會福利機構訂定第四條第八款業務終止後個人資料處理方法之措施，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。 前項措施應予記錄，並至少留存五年。但法令另有規定者，不在此限。	一、社會福利機構業務於業務終止後，自不得再繼續使用其所保有之個人資料檔案，並應作妥善處置。爰終止業務之社會福利機構，應視其終止業務之原因，將所保有之個人資料予以銷毀、刪除、移轉或其他停止處理或利用等方式處理。 二、第一項明定社會福利機構銷毀、移轉或刪除、停止處理或利用個人資料過程中，應保存處理方式、地點、時間、執行人員、接受移轉資料之對象及合法移轉依據等資料，以便日後得以提出舉證。 三、依本法第三十條規定：「損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。」爰於第二項明定銷毀、移轉、刪除、停止處理或利用個人資料之紀錄至少應留存五年。但法令另有規定者，不在此限。
第十七條　社會福利機構訂定第四條第九款個	社會福利機構應參酌相關因素，依據實

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。	務運作及法令變化等情形，檢視或修正安全維護計畫。
第十八條　社會福利機構使用資通訊系統蒐集、處理及利用個人資料時，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、個人資料檔案及資料庫之存取控制與保護監控措施。 五、外部網路入侵之防範對策。 六、非法或異常使用系統之監控及因應機制。 第一項第五款對策及第六款機制，應定期演練及檢討改善。	一、為強化資安標準規範，爰於第一項明定社會福利機構蒐集、處理及利用個人資料時，以落實個人資料安全之保障。 二、第二項明定社會福利機構應定期演練第一項第五款及第六款所定措施，以及時發現問題並檢討改善。
第十九條　社會福利機構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。	社會福利機構應完成安全維護計畫訂定之期程及主管機關得派員檢查該計畫。
第二十條　本辦法自發布日施行。	本辦法之施行日期。

附表

<table>
<tr><td colspan="4">個人資料侵害事故通報紀錄表</td></tr>
<tr><td>社會福利機構名稱</td><td colspan="3">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><td colspan="3"></td></tr>
<tr><td>事件發生時間</td><td colspan="3"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td colspan="2">個資侵害之總筆數（大約）
＿＿＿＿＿＿　筆</td></tr>
<tr><td colspan="2">□一般個資＿＿＿筆
□特種個資＿＿＿筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="3"></td></tr>
<tr><td>損害狀況</td><td colspan="3"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="3"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="3"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="3"></td></tr>
<tr><td>是否於發現個資外洩後七十二小時通報</td><td colspan="3">□是　　□否，理由</td></tr>
</table>