記帳士與記帳及報稅代理人個人資料檔案安全維護管理辦法總說明

個人資料保護法第二十七條第一項規定，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；同條第二項及第三項規定，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，其相關事項之辦法，由中央目的事業主管機關定之。

鑑於記帳士、記帳及報稅代理人為執行業務需要，保有大量個人資料，為加強記帳士、記帳及報稅代理人對於個人資料之保護措施，並建立其對個人資料之管理、稽核、保存及改善機制，爰依上開規定之授權，訂定「記帳士與記帳及報稅代理人個人資料檔案安全維護管理辦法」(以下簡稱本辦法)。其要點如下：

一、本辦法之訂定依據、適用對象、指定專人或建立專責組織及其任務。(第一條至第三條)

二、清查所保有個人資料之範圍，並建立檔案、個人資料風險評估及控管機制。(第四條及第五條)

三、個人資料安全事故之預防、通報、應變機制及財政部接獲通報之適當監督管理措施。(第六條)

四、依個人資料屬性分別訂定管理程序、告知義務之程序、委託他人蒐集、處理或利用個人資料之監督及其程序、個人資料進行國際傳輸應遵循事項、因應當事人行使權利之程序、維護個人資料正確性應採取措施、保有個人資料特定目的消失或期限屆滿之處理程序。(第七條至第十四條)

五、記帳士、記帳及報稅代理人對有關人員及資料安全之管理措施。(第十五條及第十六條)

六、以資通訊系統蒐集、處理或利用個人資料，且保有之個人資料達一萬筆者，應採行之資訊安全管理措施。(第十七條)

七、個人資料存放環境與設備安全管理措施、留存紀錄及業務終止後個人資料處理。(第十八條及第十九條)

八、個人資料安全稽核機制及整體持續檢討改善個人資料安全維護運作

機制。（第二十條及第二十一條）

九、本辦法之施行日期。（第二十二條）

記帳士與記帳及報稅代理人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　本辦法適用對象如下： 一、記帳士：指依記帳士法第二條第一項規定領取記帳士證書並執行記帳士業務者。 二、記帳及報稅代理人：指記帳士法第三十五條第一項規定之人員並執行記帳及報稅代理人業務者。 記帳士、記帳及報稅代理人應訂定個人資料檔案安全維護計畫（以下簡稱本計畫），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。 本計畫之內容應包括第三條至第二十一條規定之相關組織及程序，並應定期檢視及配合相關法令修正。	一、鑑於記帳士、記帳及報稅代理人因執行業務需要，保有大量個人資料，為維護資料之安全性與正確性，爰於第一項明定本辦法適用對象，以落實個人資料檔案之安全維護及管理。 二、依據個人資料保護法（以下簡稱本法）第二十七條第二項有關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（以下簡稱本計畫）規定，於第二項明定記帳士、記帳及報稅代理人應訂定個人資料檔案安全維護計畫。 三、第三項明定本計畫內容應包含事項。
第三條　記帳士、記帳及報稅代理人就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。 前項專人或專責組織之任務如下： 一、規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項。 二、訂定個人資料保護管理政策，將其所蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員充分瞭解。 三、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。 四、定期就執行前三款任務情形向記帳士、記帳及報稅代理人或其授權人員提出書面報告。 本計畫之訂定或修正，應經記帳士、記帳及報稅代理人或其授權人員核定。	一、配合本法施行細則第十二條第二項第一款、第七款有關配置管理之人員、相當資源與宣導及訓練等規定，於第一項明定記帳士、記帳及報稅代理人應配置相當人力、資源，以執行相關任務。 二、為利記帳士、記帳及報稅代理人善盡督導之責，於第二項明定個人資料檔案安全維護管理專人或專責組織之任務。 三、第三項明定本計畫之訂定或修正須經記帳士、記帳及報稅代理人或其授權人員核定，以利遵循，避免事後產生爭議。

第四條　記帳士、記帳及報稅代理人應清查所保有之個人資料，界定其納入本計畫之範圍並建立檔案，且應定期確認其有否變動。	配合本法施行細則第十二條第二項第二款有關個人資料安全維護措施應包括界定個人資料範圍之規定，明定記帳士、記帳及報稅代理人應定期查核及界定個人資料之範圍。
第五條　記帳士、記帳及報稅代理人應依據前條界定之個人資料範圍及其相關業務流程，分析可能產生風險，並依據風險分析結果，訂定適當管控措施。	配合本法施行細則第十二條第二項第三款有關個人資料安全維護措施應包括個人資料風險評估及管理機制之規定，明定記帳士、記帳及報稅代理人於蒐集、處理及利用過程中，應分析判斷個人資料安全可能發生之風險，俾採行適當管控措施保護個人資料，以降低風險。
第六條　記帳士、記帳及報稅代理人為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應採取下列措施： 一、採行適當應變措施，以控制事故對當事人之損害，並通報財政部。 二、查明事故之狀況並以適當方式通知當事人有關事實、因應措施及諮詢服務專線等。 三、研議預防機制，避免類似事故再次發生。 記帳士、記帳及報稅代理人遇有個人資料安全事故時，應自發現事故時起算七十二小時內，檢附「個人資料侵害事故通報及紀錄表」(如附表)，以電子郵件方式向財政部通報，並應視案情發展適時通報處理情形，以及將整體查處過程、結果及檢討等函報財政部。 財政部收受前項通報後，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。	一、配合本法施行細則第十二條第二項第四款有關個人資料安全維護措施應包括事故之預防、通報及應變機制之規定，於第一項明定記帳士、記帳及報稅代理人應採取之因應措施，以降低或控制損害，並讓當事人瞭解相關狀況，使當事人能採取相關措施防止損害發生或擴大，並應研議預防機制，防杜事故重複發生。 二、依行政院及所屬各機關落實個人資料保護聯繫作業要點第四點第一項第三款有關本辦法應包括非公務機關個資外洩時應通報之對象、時點、應通報事項、後續行政檢查等事項規定，於第二項明定記帳士、記帳及報稅代理人遇個人資料安全發現事故後，應依附表格式於七十二小時內通報財政部。 三、第三項明定財政部於接獲記帳士、記帳及報稅代理人通報後，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。
第七條　記帳士、記帳及報稅代理人應依個人資料屬性，分別訂定下列管理程序： 一、確認蒐集、處理或利用之個人資料是否包含本法第六條所定個人資料及其特定目的。 二、確保蒐集、處理或利用本法第六條所定個人資料符合相關法令之要件。 三、非本法第六條所定個人資料，如認	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應依個人資料之屬性訂定管理程序。

為具有特別管理之需要，得訂定特別管理程序。	
第八條　記帳士、記帳及報稅代理人為遵守本法第八條及第九條關於告知義務之規定，應採取下列方式： 一、檢視蒐集、處理或利用個人資料之特定目的，除符合法定免為告知事由外，均應依法告知當事人相關事項。 二、依資料蒐集之情況，採取適當之告知方式。	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應遵循本法第八條及第九條規定有關非公務機關蒐集、處理或利用個人資料之告知義務。
第九條　記帳士、記帳及報稅代理人蒐集、處理個人資料應符合本法第十九條第一項規定，具有特定目的及法定要件。 記帳士、記帳及報稅代理人利用個人資料應依本法第二十條第一項規定，於特定目的必要範圍內利用；於特定目的外利用個人資料時，應具備法定特定目的外利用要件。	一、配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，於第一項明定記帳士、記帳及報稅代理人應遵循本法第十九條規定有關蒐集或處理個人資料應符合特定目的及法定要件。 二、第二項明定記帳士、記帳及報稅代理人應遵循本法第二十條規定有關利用個人資料應符合特定目的必要範圍，及法定特定目的外利用要件。
第十條　記帳士、記帳及報稅代理人委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項及方式。	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應遵循本法施行細則第八條規定有關委託他人蒐集、處理或利用個人資料之監督責任。
第十一條　記帳士、記帳及報稅代理人將當事人個人資料作國際傳輸者，應檢視是否受財政部限制，並應告知當事人其個人資料所欲國際傳輸之區域，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。	依本法第二十一條規定，中央目的事業主管機關得限制非公務機關對於個人資料進行國際傳輸，並配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人將當事人個人資料作國際傳輸者，應檢視是否受財政部限制，並告知當事人其個人資料所欲國際傳輸之區域，及對資料接收方為適當之監督。
第十二條　記帳士、記帳及報稅代理人受理當事人就其個人資料行使本法第三條規定權利，應採取下列措施： 一、確認其為個人資料之本人，或經個人資料之本人委託授權。 二、提供當事人行使權利之方式，並遵	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應遵循本法第三條有關當事人行使權利之規範。

守本法第十三條有關處理期限規定。 三、如酌收必要成本費用應予告知。 四、具本法第十條但書及第十一條第二項但書、第三項但書規定得拒絕當事人行使權利之事由，應附理由通知當事人。	
第十三條　記帳士、記帳及報稅代理人為維護其所保有個人資料之正確性，應採取下列方式： 一、於蒐集、處理或利用過程檢視個人資料正確性。 二、發現個人資料不正確時，適時更正或補充，並通知曾提供利用之對象。 三、個人資料正確性有爭議者，依本法第十一條第二項規定處理。	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應遵循本法有關維護保有個人資料正確性之規範。
第十四條　記帳士、記帳及報稅代理人應定期確認保有個人資料之特定目的及期限，如特定目的消失或期限屆滿時，應依本法第十一條第三項規定處理。	配合本法施行細則第十二條第二項第五款有關個人資料安全維護措施應包括個人資料蒐集、處理及利用之內部管理程序規定，明定記帳士、記帳及報稅代理人應遵循本法第十一條第三項有關特定目的消失與期限屆滿之處理規定。
第十五條　記帳士、記帳及報稅代理人應採取下列人員管理措施： 一、依據作業之需要，建立管理機制，設定所屬人員不同權限，並定期確認權限內容之適當性及必要性。 二、指定各相關業務流程涉及蒐集、處理或利用個人資料之負責人員。 三、與所屬人員約定保密義務。 四、所屬人員離職時，持有之個人資料應辦理交接，不得於離職後繼續使用，並簽署保密切結書。	配合本法施行細則第十二條第二項第六款有關個人資料安全維護措施應包括人員管理之規定，明定記帳士、記帳及報稅代理人應採行之人員管理措施。
第十六條　記帳士、記帳及報稅代理人應採取下列資料安全管理措施： 一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒體規範。 二、保有之個人資料內容如有加密需要，應於蒐集、處理或利用時，採取適當加密機制。 三、作業過程有備份個人資料需要時，比照原件，依本法規定予以保護。	配合本法施行細則第十二條第二項第六款有關個人資料安全維護措施應包括資料安全管理之規定，明定記帳士、記帳及報稅代理人應採行之資料安全管理措施。

四、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、電腦、自動化機器設備或其他存放媒介物報廢或轉作其他用途時，採適當防範資料外洩措施。	
第十七條　記帳士、記帳及報稅代理人因執行業務以資通訊系統蒐集、處理或利用個人資料筆數達一萬筆者，應採行下列資訊安全措施： 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。 記帳士、記帳及報稅代理人保有個人資料筆數未達一萬筆，於本條文施行後，因直接或間接蒐集而達一萬筆者，應於保有筆數達一萬筆之日起算六個月內採行前項資訊安全措施。 第一項第五款及第六款所定措施，每年應至少辦理一次演練並檢討改善。	一、配合行政院及所屬各機關落實個人資料保護聯繫作業要點第四點第一項第二款有關非公務機關使用資通訊系統蒐集、處理或利用個人資料應加強管理措施之規定，於第一項明定記帳士、記帳及報稅代理人以資通訊系統蒐集、處理或利用個人資料筆數達一萬筆者，應採行之資訊安全措施。 二、第二項明定保有個人資料未達一萬筆，於本條文施行後，因直接或間接蒐集而達一萬筆者，給與記帳士、記帳及報稅代理人六個月緩衝期採行資訊安全措施。 三、為使記帳士、記帳及報稅代理人以資通訊系統蒐集、處理或利用之個人資料檔案遭遇各類資安事件時，能儘速恢復正常並控制損害，爰於第三項明定應針對防範非法入侵或異常使用等應變措施每年應至少辦理一次演練並檢討改善。
第十八條　記帳士、記帳及報稅代理人保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物，應採取下列環境及設備安全管理措施： 一、針對存放儲存媒介物之環境，實施適當進出管制措施。 二、依儲存媒介物之特性及使用方式，建置適當保護設備或技術。 三、依所屬人員業務特性、內容及需求，訂定適當管理措施。	配合本法施行細則第十二條第二項第八款有關個人資料安全維護措施應包括設備安全管理之規定，明定記帳士、記帳及報稅代理人應採行之環境及設備安全管理措施。
第十九條　記帳士、記帳及報稅代理人應採行適當資料安全維護措施，採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供必要時說明其所定本計畫執行情況。 記帳士、記帳及報稅代理人對於業務終止後保有之個人資料，應依下列方式處理，並留存相關紀錄：	一、配合本法施行細則第十二條第二項第十款有關個人資料安全維護措施應包括使用紀錄、軌跡資料及證據保存之規定，明定記帳士、記帳及報稅代理人應留存相關軌跡紀錄，以明確個人資料使用歷程情形，避免爭議。 二、本法第三十條規定損害賠償請求權，應自損害發生時起五年內行使，為避

一、銷毀：銷毀之方法、時間、地點及證明銷毀方式。 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。 前二項所定之紀錄、軌跡資料及相關證據，應至少留存五年。	免發生損害請求賠償時，相關紀錄已遭記帳士、記帳及報稅代理人提前銷毀，爰明定應至少留存五年。
第二十條　記帳士、記帳及報稅代理人應訂定個人資料安全稽核機制，定期或不定期查察是否落實執行本計畫所定相關事項。	配合本法施行細則第十二條第二項第九款有關個人資料安全維護措施應包括資料安全稽核機制之規定，明定記帳士、記帳及報稅代理人應訂定個人資料安全稽核機制，以利落實執行相關規範。
第二十一條　記帳士、記帳及報稅代理人應參酌執行業務現況、社會輿情、技術發展、法令修正等因素，檢視本計畫合宜性，必要時應予修正。	配合本法施行細則第十二條第二項第十一款有關個人資料安全維護措施應包括個人資料安全維護之整體持續改善之規定，明定記帳士、記帳及報稅代理人應參酌執行業務現況、社會輿情、技術發展、法令修正等因素，適時檢討修正本計畫，俾利持續改善個人資料安全維護運作機制。
第二十二條　本辦法除第六條自發布日施行外，自發布後六個月施行。	為利記帳士、記帳及報稅代理人因應調適，有提供緩衝期之必要，爰除第六條外，明定自發布後六個月施行；至第六條有關個人資料安全事故之預防、通報及應變規定刻不容緩，爰明定自發布日施行。

附表

<table>
<tr><td colspan="3">個人資料侵害事故通報及紀錄表</td></tr>
<tr><td>記帳士（記帳及報稅代理人）
事務所名稱：

姓名：</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽章
職稱：
電話：
電子郵件：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></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>個資侵害之總筆數（大約）＿＿＿筆</td></tr>
<tr><td>□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="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後72 小時內通報</td><td colspan="2">□是
□否，理由</td></tr>
</table>