_____記帳及報稅代理人個人資料檔案安全維護計畫 （範本）

壹、記帳及報稅代理人事務所之組織及規模

一、名稱：_____**記帳及報稅代理人事務所**

二、事務所地址：

三、負責人：

四、員工人數：　　人

貳、個人資料檔案安全維護管理措施

第一條：依據個人資料保護法第 27 條第 3 項及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第 2 條規定辦法，爰訂定「個人資料檔案安全維護計畫」(下稱本計畫)。

第二條：目的為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本事務所員工應依本計畫辦理個人資料檔案安全管理及維護事宜。

本計畫應包含管理辦法第 3 條至第 21 條規定相關組織及程序。

應定期檢視本計畫及配合相關法令修正。

第三條：本維護計畫書指定之專責人員姓名：_____。

預算：每年新台幣_____元。。(包含管理薪資、設備費用等，可記載一定範圍之金額，或依實際狀況填寫)

專責人員任務如下：

1. 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宜。
2. 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，公告使本事務所員工充分瞭解。
3. 定期對本事務所員工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、責任範圍及各種個人資料保護事項之方法或管理措施。
   (1)每年至少進行一次個人資料保護相關法規宣導及教育訓練至少**一小時**，使本事務所人員知悉應遵守之規定，並留存相關紀錄（例如：簽名冊等文件)。
   (2)對於新進人員應特別給予指導，使其明瞭個人資料保護相關法規、責任範圍及應遵守之管理措施。
4. 定期就執行前開任務情形向負責人或其授權人員提出書面報告。
5. 本計畫之訂定或修正，應經記帳及報稅代理人或其授權人員核定。

6.遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第四條：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。且定期確認上述內容是否異動。

第五條：依個人資料範圍及其業務流程可能產生的風險：

1.經由本事務所電腦下載或外部網路入侵而外洩。

2.經由接觸書面契約而外洩。

3.員工及第三人故意竊取、毀損或洩漏。

可能產生的風險訂定適當管控措施：

1.每位員工均應以其使用者代碼及密碼登入事務所電腦,並定期進行網路資訊安全維護及控管。

2.列冊管理書面契約，落實員工查(調)閱書面契約紀錄管理。

3.加強員工管理及事務所出入人員管制。

第六條：發現本事務所有個人資料遭竊取、竄改、毀損、滅失或洩漏等事故，應採取下列措施：

1.應立即通報負責人並查明發生原因及責任歸屬,及依實際狀況採取相關應變措施，以控制事故對當事人之損害。

2.對於個人資料遭竊取、竄改、毀損、滅失或洩漏之當事人，應以適當方式通知當事人,使其知悉及本事務所持有個人資料發生事故、已採取之處理措施、諮詢服務電話及聯絡窗口等資訊。

3.針對事故發生原因研議預防機制，避免類似事故再次發生。

本事務所應自發現事故時起算 72 小時內，填具「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，並將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。

第七條：本事務所依個人資料屬性，分別訂定下列管理程序：

1.應確認蒐集、處理或利用之個人資料是否包含個人資料保護法第 6 條所定個人資料及其特定目的。

2.並確保蒐集、處理或利用個人資料保護法第 6 條所定個人資料符合相關法令之要件。

3.非個人資料保護法第 6 條所定個人資料，如認為具有特別管理之需要，訂定特別管理程序。

第八條：特定目的為會計與相關服務(129)、人事管理(002)。

1.蒐集、處理或利用個人資料之特定目的，均依法告知當事人相關事

項。本事務所直接向當事人蒐集個人資料時，應明確告知以下事項：

(1)事務所名稱。

(2)蒐集目的。

(3)個人資料之類別。

(4)個人資料利用之期間、地區、對象及方式。

(5)當事人得請求閱覽、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，及不提供將對其權益之影響。

2. 本事務所之告知方式，包括言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉等方式。

3. 本事務所蒐集非由當事人提供之個人資料，應於處理或利用前向提供人告知個人資料應告知之事項，若 提供人表示拒絕提供，應立即停止處理、利用其個人資料。

4. 本事務所與當事人簽訂之委託書，如獲得當事人書面同意，得進行個人資料蒐集、處理及利用，並於委託期限屆滿時主動刪除或銷毀。但因法令規定或執行業務所必須或經客戶書面同意者，不在此限。

第九條：本事務員工因執行業務而蒐集、處理個人資料時，應檢視是否符合個人資料保護法第 19 條第 1 項之特定目的及法定要件。

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，應檢視是否符合個人資料保護法第 20 條第 1 項但書情形。

第十條：本事務所如委託他人蒐集、處理或利用個人資料之全部或一部時，對受託者應為適當之監督，並明確約定相關監督事項及方式。

第十一條：本事務所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. 當事人行使個人資料保護法第 3 條所定權利之相關事項。

第十二條：當事人可行使的權利：

1. 應依當事人之請求，就其個人資料得查詢或請求閱覽、製給複製本、補充、更正、停止蒐集、處理或利用或請求刪除，本事務所不得請其預先拋棄或以特約限制之。應確認其為個人資料之本人，或經個人資料之本人委託授權。

2. 提供當事人行使權利之方式，並遵守個人資料保護法第 13 條有關處

理期限規定。

3. 如酌收必要成本費用應予告知。

4. 當事人就其個人資料行使權利事項如有個人資料保護法第 10 條但書、第 11 條第 2 項但書及第 3 項但書規定得拒絕當事人行使權利之事由，本事務所應附理由通知當事人。

第十三條：維護個人資料正確性之方式：

1. 於蒐集、處理或利用過程應檢視個人資料正確性。

2. 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。

3. 個人資料正確性有爭議者，主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

第十四條：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，主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

第十五條：人員管理措施：

1. 本事務所依員工（例如主管、非主管人員）之業務需求設定不同之個人資料使用權限,並定期(每年至少 1 次)確認權限內容之適當性及必要性。本事務所依業務流程指定個人資料蒐集、處理或利用之負責人員，相關負責個人資料檔案管理人員於職務異動時，應移交其保管之檔案資料，接辦人員應另行設定密碼。

2. 如因業務需要須利用非權限範圍之個人資料時，應事前提出申請，經業務主管人員同意後開放權限利用。此項業務之連絡窗口為：_____；電話：_____，並將聯絡窗口及電話等資料，揭示於本事務所營業處所佈告欄或網頁。

3. 本事務所與員工之勞務契約應納入「員工就於任職期間因業務所接觸個人資料均負保密義務」之相關保密條款。

4. 員工離職時，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。

第十六條：資料檔案安全管理措施：

1. 員工如因其工作執掌而須使用事務所電腦輸出、輸入個人資料時，均須鍵入其使用者代碼及密碼，同時在使用範圍及使用權限內為之。

2. 本事務所員工使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，其帳號密碼應保密，不得洩漏或與他人共用，

密碼應每六個月變更，並於變更密碼後始可繼續使用電腦。

3. 本事務所人員應妥善保管個人資料之儲存媒介物，執行業務時應依個人資料保護法規定蒐集、處理及利用個人資料。

4. 加強管控本事務所員工對內或對外之個人資料傳輸，避免外洩。

5. 非主辦業務之員工查閱契約書類時，應經負責人或其授權人員之同意。

6. 以書面資料儲存個人資料者，應設置專屬儲存空間並列冊管理。

7. 書面資料儲存空間應指派專人管理管理，並將調閱或使用個人資料情形作成書面紀錄，且事務所員工非經負責人或其授權人員同意不得任意複或影印資料。

8. 書面資料儲存空間應設置防火設備或其他相關防護措施設備，以防止資料滅失或遭竊取。

9. 以書面資料儲存之個人資料，於銷毀前應以碎紙設備進行處理。

第十七條：本事務所使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上時，採取下列資訊安全措施：

1. 使用者身分確認及保護機制。

2. 個人資料顯示之隱碼機制。

3. 網際網路傳輸之安全加密機制。

4. 個人資料檔案與資料庫之存取控制及保護監控措施。

5. 防止外部網路入侵對策。

6. 非法或異常使用行為之監控及因應機制。

因直接或間接蒐集而達一萬筆時，應於保有筆數達一萬筆之日起算 6 個月內採行前項資訊安全措施。

第一項第 5 款至第 6 款所定措施，每年至少辦理一次演練並檢討改善。

第十八條：運用電腦及儲存媒介儲存個人資料管理

1. 指派專人管理用於儲存個人資料之電腦，本事務所員工應以其專屬帳號密碼登入使得使用電腦，並留存使用紀錄；該電腦不得作為公眾查詢之前端工具。

2. 用於儲存個人資料之電腦，應安裝防毒軟體、定期掃毒，並定期進行電腦保養維護，於保養維護或更新設備時，應注意資料之備份及相關安全措施。

3. 指派專人管理用於儲存個人資料之儲存媒介，儲存媒介使用完畢應即退出不得任意放置在電腦，並就其使用情形作成書面紀錄。

4. 用於儲存個人資料之儲存媒介非經負責人或其授權人員同意並作成

紀錄不得攜帶外出或拷貝複製。

5.運用電腦及儲存媒介儲存之個人資料應定期(例如：每月)備份，並比照原件予以保護。

6.儲存個人資料之電腦及儲存媒介於報廢、汰換或轉作其他用途前，應由本事務所負責人或其授權人員檢視各該設備儲存之個人資料是否確實刪除。

7.重要個人資料應另加設管控密碼,非經陳報負責人或經指定之管理人員核可，並取得密碼者，不得存取。

8.於放置電腦及儲存媒介之空間設置防火及其他相關防護措施設備,以防止資料滅失或遭竊取。

第十九條：應採行適當資料安全維修措施，採個人資料使用紀錄、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。

對於業務終止後保有之個人資料，依下列方式處理：

1.銷毀：銷毀之方法、時間、地點及證明銷毀方式。

2.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。

3.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。

前二項紀錄、軌跡資料及相關紀錄應至少留存 5 年。

第二十條：本事務所定期(每年至少 1 次)辦理個人資料檔案安全維護稽核，檢查本事務所是否落實本計畫規範事項，針對檢查結果不符合及潛在風險事項規劃改善措施，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.確認不符合事項之內容及發生原因。

2.提出改善及預防措施方案。

3.紀錄檢查情形及結果。

前項檢查情形及結果應載入稽核報告中，由事務所負責人簽名確認。

第廿一條：本計畫應參酌執行業務現況、社會輿情、技術發展、法令修正等因素，檢視其合宜性，並經負責人或其授權人員於核定後予以修正。

第廿二條：本計畫書訂定於 111 年 07 月 20 日

本計畫書第一次修訂於 112 年 12 月 31 日

附表：個人資料侵害事故通報及紀錄表

個人資料侵害事故通報及紀錄表

<table>
<tr><td>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>

財政部(賦稅署)通報聯繫窗口

電子郵件：dot_ycchen@mail.mof.gov.tw

聯絡電話：(02)23228000分機8199