機密等級：內部文件

農業部
桃園區農業改良場

個人資料使用紀錄、稽核軌跡及證據保存指引

第 1.0 版

113 年 8 月 22 日 頒行

目錄

壹、目的

本場各單位業務執行過程中，涉及個人資料蒐集、處理或利用情形時，對個人資料檔案所執行之作業應留存相關之使用紀錄與稽核軌跡；發生個人資料被竊取、竄改、毀損、滅失或洩漏等事件時，本場應協助進行證據保存，以利專業人員能依據保存之資料，進行蒐證並還原事件真相，保障業務承辦與個資當事人權益。

貳、適用範圍

一、組織與業務

本指引適用於本場涉及個人資料蒐集、處理、利用、傳輸、銷毀之相關業務。

二、個人資料檔案

涵蓋資訊紀錄、資訊系統其型式可為電子檔案、系統化資料庫、紙本等，如下列參考類別與項目(但不限於下表所列項目)：

資產類別	個資檔案**範例**(不限於本表所列項目)	
資訊紀錄	●人事資料庫、資料檔 ●保險資料 ●考試分發人員基本資料 ●同仁在離職證明書/服務證明書 ●廠商通訊錄 ●研討會/教育訓練報名表	●約聘僱人員契約書 ●公務人員派免令 ●甄審、進修暨考績甄審委員會委員名單 ●公務人員訓練、進修資料 ●保密切結書 ●學員/農友名冊
資訊系統	●人事管理資訊系統 ●政府歲計會計資訊管理系統	●土壤肥力與作物營養診斷服務查詢系統

參、名詞定義

一、個人資料

指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案

指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、稽核日誌

稽核日誌係指對非原保存資料檔案，使用自動或非自動化方式對使用者活動、異常、系統或資通安全事件所留存之紀錄。

四、使用紀錄

不同類別之使用者對個人資料檔案所進行的各項作業所留存的存取行為紀錄。針對不同層面，使用紀錄可區分為:

(一) 營運流程

各業務流程中，針對個人資料檔案申請、簽核及核准之資料存取及授權行為紀錄。

(二) 應用系統

透過應用系統介面存取個人資料檔案之行為紀錄。

(三) 資料庫管理

連線資料庫進行操作及存取行為之使用紀錄。

(四) 作業系統

由系統主機上進行相關作業系統各項操作之使用紀錄，或是在個人電腦中存取相關檔案之行為紀錄。

(五) 網路管理

存取網路環境與相關設備之紀錄，如網路流量監控紀錄、網路安全事件封包紀錄或相關網路設備之操作監控紀錄。

(六) 實體環境

存取實體環境之紀錄，如門禁管理系統出入紀錄、監視系統影像紀錄。

五、 稽核軌跡

係指個人資料在蒐集、處理、利用過程中，所產生非屬於原蒐集個資本體之衍生資訊(Log Files)，包括(但不限於)資料存取人之代號、存取時間、使用設備代號、網路位址(IP)、經過之網路路徑…等。

資訊系統與儲存資料發生之活動或事件紀錄，作為比對、查證資料存取用途時，必須另外提供有關處理細節之資料，包含資訊儲存的日期、在不同的媒體之間移動或轉換的過程、系統運作之控管方式等，這些細節資料可稱為稽核軌跡。

肆、作業程序

一、 權責

(一) 個人資料保護管理執行小組(以下簡稱本小組)

1. 審核本指引。
2. 提供適當資源，以利使用紀錄、軌跡資料與證據能順利保存。

(二) 本小組執行秘書

1. 督導各單位依本指引保存相關資料。
2. 陳報查核結果予個人資料保護管理執行小組。

(三) 本小組委員

1. 督導該單位依本指引保存相關資料。
2. 審核該單位必須留存之使用紀錄與稽核軌跡項目
3. 審核、授權使用相關紀錄與軌跡資料。

(四) 各單位個人資料保護專責人員

1. 宣導本指引規定
2. 宣導個資與資安防護相關規定。
3. 發生個資事件，協助證據蒐集、保存與調查。

(五) 各單位個資業務承辦

1. 擬定各單位必須留存之使用紀錄與稽核軌跡項目。
2. 產生、蒐集與保存各項使用紀錄與軌跡資料。
3. 發生個資事件，負責證據蒐集、保存與調查。

(六) 資訊/個資專責單位

1. 維運本場系統儲存設備，以保存使用紀錄與軌跡資料並定期備份。
2. 提供本場外部系統之建置與維運諮詢。
3. 發生個資事件，提供必要之諮詢與協助。

二、 執行時機

(一) 定期：依據各業務流程進行

(二) 不定期：當下列事件發生時須執行證據蒐集：

1. 發生個人資料被竊取、竄改、毀損、滅失或洩漏等事件。
2. 發生訴願或賠償請求事件。

伍、使用紀錄與稽核軌跡保存

一、 一般原則

(一) 使用紀錄、存取歷史活動或事件應被記錄與保存，以便可重建並作為客觀證據。

(二) 稽核軌跡資料應記錄足夠資訊，以利作為查證之證據。

(三) 使用紀錄與稽核軌跡包含系統跟操作人員產生的紀錄檔(log)。

(四) 資料蒐集或匯入系統時的關鍵資訊應記錄於稽核軌跡資料。

(五) 日期與時間

1. 稽核軌跡資料應有相關事件之日期與時間。
2. 記載事件日期與時間必須正確，以便後續調查決定發生順序。
3. 稽核軌跡資料若由系統自動建立，應在事件記錄後立刻產出。

(六) 稽核軌跡資料可能會被多個單位存取，應經由主要負責單位同意。

(七) 變更管制

對系統或檔案進行變更，應確保

1. 對儲存於系統的資訊所進行之變更被記錄。
2. 建立並保存軌跡資料，識別改變的性質、人員、地點、自動變更的系統、啟動變更的程式等。

3. 保存前一版本，以便可識別出變更。

(八) 作業流程

1. 新的作業流程被定義或原有流程改變，應加以記錄。
2. 採用系統產生時，稽核軌跡資料產生的時點應被定義。
3. 系統需可由經授權的使用者選擇特定的時點資料。
4. 處理流程應記錄足夠資訊以資辨識。

二、使用紀錄與稽核軌跡之處理

(一) 產生

1. 稽核軌跡應盡量由系統自動產生。
2. 若稽核軌跡非由系統自動產生時，應將產生的過程記載於相關手冊或表單中。
3. 稽核軌跡資料檔之容量滿載時，應將採取之相關處理程序記在於手冊或表單中。

(二) 保存

1. 稽核軌跡資料應視為文件化資訊進行保存。
2. 稽核軌跡資料之保存期限至少應與參考該軌跡資料資訊之保存期間一致。原則上以 5 年為宜。

(三) 存取

1. 稽核軌跡資料存取與解讀方式應描述於相關之手冊
2. 稽核軌跡資料於必要時，應可由經授權之外部人員進行調查。

(四) 安全防護

1. 應防止對內容之變更
2. 應依據安全相關規範進行保護
3. 應有安全之備份
4. 必須進行檔案復原程序時，應留存足夠之資訊以證實復原不影響稽核軌跡資料之可辨識性。
5. 紙本之軌跡資料應置於安全位置保存。

三、使用紀錄與稽核軌跡資料移轉

(一) 系統的稽核軌跡資料應可辨識出相關的處理與事件的日期時間。

(二) 資訊由儲存裝置移轉到其他裝置時，應有資料檔案移轉程序，並應記錄於稽核軌跡資料。

(三) 檔案轉換格式時，轉換之細節應紀錄於稽核軌跡資料。

四、使用紀錄與稽核軌跡資料刪除

(一) 使用紀錄與稽核軌跡蒐集後，若需刪除原始文件應加以記錄。

(二) 保存期限到期後，刪除應加以記錄。

陸、證據蒐集與保存

本場發生個資侵害事件時，個資專責單位應協助進行蒐證、調查與鑑識，儘速釐清事件真相，提供包含個人資料檔案相關使用紀錄與稽核軌跡等資料。

一、 一般原則

(一) 發生個資侵害事件，為釐清事件真相，須進行數位鑑識流程，數位鑑識大致可以分成四個階段，分別是蒐集、檢視、分析和證據呈現。本場應協助進行證據蒐集。

(二) 為了確保蒐證過程的嚴謹，必須由專業受過鑑識訓練的專業人員進行，確保蒐集到的證據具有證據能力和證明力。

(三) 個人資料保護法本身的罰則仍有刑責的部分，為了確保證據能力和證明力，需依嚴謹的刑事訴訟法進行蒐證，確保後續的證據效力。

二、 蒐證與保存

「證據保全」是蒐證過程最重要的精神所在，個人資料保護法施行細則第 12 條規定的 11 項安全維護措施中，本場應確實實施並留存管理流程與系統之相關紀錄。為提供後續的鑑識分析，必須蒐集所需要的數位與紙本證據，包括各種 Log 檔，或者是各種數位或紙本文件，甚至是各種系統的資料內容等。相關作業分為事前、事中和事後等三個階段：

(一) 事前證據保留

1. 經評估應保存之項目，進行相關的設定、安全控管，和完整、定期的備份機制並保留各種軌跡資料。
2. 為使證據有分析的效果，應保存包括來源 IP、使用者是誰、在什麼時間點存取哪些系統，在相關系統內做了什麼事情的行為紀錄。

(二) 事中證據保存

1. 遭遇到大量的異常存取或攻擊事件，被攻擊過程應持續記錄，這些證據保存有助釐清資安事件的問題根源所在。
2. 數位證據的蒐證須經由第三方單位，或者具有鑑識專業能力的人員執行。
3. 面臨異常事件時，應進行封包擷取側錄，並尋求專業的鑑識團隊，協助進行相關的數位證據蒐證。
4. 保存過程應確保證據「不被竄改」。

(三) 事後證據擷取

1. 事前完整的證據保留，事中證據保存，到事後，針對所需的證據進行擷取即可。
2. 進行蒐證時，相關單位須協助提供特定個人或某個系統的資料。