機密等級：內部文件

農業部
桃園區農業改良場

個人資料隱私衝擊分析及風險管理程序

第 1.0 版

113 年　8　月　22　日　　頒行

目錄

壹、目的

將建立之個資盤點清冊，依其業務與系統特性，釐清可能面臨的風險，對於本場違反法令與安全維護事項不足之風險加以控管，確保本場依個人資料保護法之要求，避免人格權受侵害，與促進個人資料之合理利用；另依風險程度之差異，辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

貳、適用範圍

一、組織與業務

本程序適用於全場涉及個人資料蒐集、處理、利用、傳輸、銷毀之相關業務與系統。

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**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 ●評審委員名單 ●廠商通訊錄 ●研討會/教育訓練報名表	●契約 ●保密切結書 ●同仁在離職證明書/服務證明書 ●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。

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. 決定可接受風險等級。
2. 審核個資風險評鑑報告與風險處理計畫。
3. 提供資源使風險管理活動能順利進行。

(二) 本小組執行秘書

1. 督導個資盤點與風險管理措施。
2. 督導風險處理計畫之執行，以確認風險降至可接受風險等級，同時符合管理政策與程序。

(三) 本小組委員

1. 審核各業務承辦人所提列之個資檔案清冊。
2. 審核各業務承辦人的風險評鑑結果、風險處理計畫及執行結果。

(四) 各單位個人資料保護專責人員

1. 檢視各業務承辦人所提列之個資檔案清冊。
2. 針對提列的個資檔案、鑑別其重要性與衝擊。
3. 彙整各業務承辦人的風險評鑑結果。
4. 針對風險評鑑結果訂定風險處理計畫。
5. 追蹤風險處理計畫執行結果。

(五) 各單位保有個資業務承辦人

1. 執行隱私衝擊分析。
2. 執行風險評鑑，並鑑別潛在風險與所需之安控機制。

(六) 個資/資安專責單位

1. 資安防護技術支援。
2. 彙整各業務承辦人的風險評鑑結果，並提供改善建議後產出風險評鑑報告。

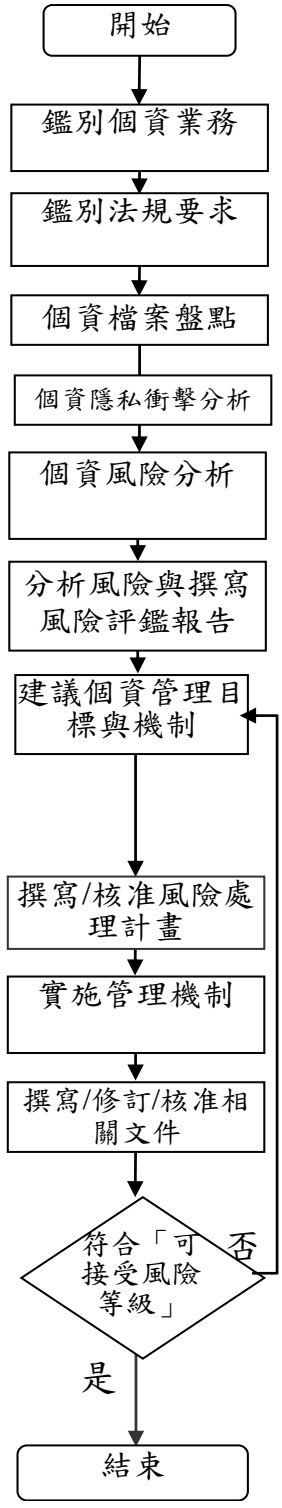
二、 執行時機

(一) 定期：每年一次

(二) 不定期：當下列事件發生時須執行個人資料風險評鑑：

1. 個資相關業務有重大改變。
2. 本場組織架構重大改變。
3. 重大個資事件發生。

三、個資風險管理流程

流程	說明
	●依據各單位業務，鑑別本場個資相關業務。 ●鑑別本場應遵循之個資相關法規與主管機關要求。 ●依業務盤點列出個資檔案與個資運用狀況。 ●評估個資檔案之重要性與可能衝擊，個資檔案重要等級。 ●鑑別個資檔案相關業務/系統的威脅與脆弱點，並鑑別發生之可能程度。 ●計算風險值，並斷定其風險等級。 ●分析風險評鑑結果，並撰寫個資風險評鑑報告。 ●針對各項不可接受風險採取如下措施： – 釐清管理需求 – 考量本場內相關之安控需求 – 選定新的管理目標與安控機制 ●撰寫風險處理計畫，並陳送個人資料保護管理執行小組核准實施。 ●實施新的安控機制，量測目標達成情形，以確保控制措施有效。 ●撰寫/修訂相關文件，並陳送個人資料保護管理執行小組核准頒行。 ●依據風險處理計畫，再次評估先前鑑別之風險，以確定符合「可接受風險等級」。

伍、個資風險管理流程說明

一、鑑別個資業務

由各單位業務活動中，鑑別是否涉及個人資料蒐集、處理、利用、傳輸、銷毀？若有，

則應進行後續管理作業。

二、個資保護法規與要求分析

已鑑別之個資業務流程中，本場同仁應遵守之個資相關法令、合約及協議。如:

(一) 個人資料保護法。

(二) 個人資料保護法施行細則。

(三) 主管機關要求之相關規定。

(四) 與廠商或相關團體因執行業務所訂定之合約或協議。

(五) 單位或內部自行訂定之規定。

(六) 本場資通安全政策。

(七) 本場個人資料保護及隱私管理政策。

三、個資檔案盤點

盤點業務活動中相關的個資檔案項目,並建立個資檔案清冊,鑑別個資管理之相關資訊，包含下列項目(各項目填寫方式請參考「個人資料盤點及維護管理程序」附錄之個資盤點清冊填寫說明):

(一) 檔案名稱

(二) 檔案形態 (如紙本、電子檔、資料庫)

(三) 個資類別

(四) 個資項目

(五) 特種資料 (Y/N)、高風險資料 (Y/N)

(六) 資料所屬單位、保管單位、保管人員、使用之相關業務或系統

(七) 保有依據、保有業務目的 (特定目的)

(八) 資料來源 (蒐集對象)、資料蒐集方法

(九) 內部作業流程

(十) 保存期限

(十一) 資料分享單位、資料外部傳輸方法、內部資料傳輸方法

(十二) 資料儲存環境/保管場所

(十三) 涉及個資委外作業(Y/N)

(十四) 銷毀方式

四、 個資隱私衝擊分析

針對本場個資檔案項目，依據其個資含量、個資數量、個資運用等特性，評鑑個資檔案項目的重要等級。重要等級判斷依據如下表。重要等級如下表:

評等	條件	說明
4	含有特種個人資料。	符合左列任一條件即為 4
	個資保管數量逾 30,001 筆以上。	
	提供外部運用：提供外部廠商者，若管理不當，有大量外洩之虞。	
3	**含高風險個資項目**。包括弱勢族群(隔代教養/低收入戶/身障/肢障等)、身心狀況(精神耗弱)、個人銀行帳戶、其他財務資訊、信用卡卡號、個人特徵的詳細說明、對個人將產生負面影響的資訊。	符合左列任一條件即為 3
	個資保管數量逾 5,001 筆~30,000 筆以內。	
	提供外部網站運用：例如：該系統於外網可使用，有遭駭客攻擊之虞。	
2	**一般個資項目超過 5 項**：姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、婚姻、家庭、教育、職業、聯絡方式、社會活動等達 6 項(含)以上者。	符合左列任一條件即為 2
	個資保管數量逾 1,001 筆~5,000 筆以內。	
	機關內部跨單位或供外部政府機關運用：僅提供機關內部之不同單位或外部政府機關運用者。	
1	**一般個資 5 項以內者**：姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、婚姻、家庭、教育、職業、聯絡方式、社會活動等達 5 項(含)以內者。	符合左列任一條件即為 1
	個資保管數量 1,000 筆以內。	
	個人或單位內運用：僅個人或同一單位運用者。	

五、 若個人資料檔案項目之重要性等級為 3 或 4 者，應合併其業務或系統後，再以業務或系統，依據本程序「個人資料隱私衝擊分析及風險管理程序」，進行下一步驟之個資風險分析。針對個人資料檔案項目之重要性等級為 1 或 2 之業務或系統，則不再進行下一步驟之個資風險分析。

六、 個資風險分析

(一) 每個重要性等級為 3 或 4 之業務或系統，均應評鑑第陸章附錄威脅/脆弱點相關資訊所列示之所有風險，並鑑別其威脅等級與脆弱點等級。

(二) 威脅等級

指威脅發生的機率或可能性。評等原則如下表:

威脅發生可能性	評等	分級原則	說明
高	3	每年發生 7 次(含)以上 事件或威脅沒發生過，但有可能發生，且每月人為阻止每月 4 次(含)以上。	符合左列任一條件即為 3
中	2	每年發生 3~6 次 事件或威脅沒發生過，但有可能發生，且人為阻止每月達 1~3 次。	符合左列任一條件即為 2
低	1	每年發生 2 次(含)以內 事件或威脅沒發生過，但有可能發生，或人為阻止每月不到 1 次。	符合左列任一條件即為 1

人為阻止：係指因為人為注意而阻止外來威脅所產生的資安事件。

機關內部人員發現：以人為阻止方式之次數來概估。

機關外部人員發現：以實際發生事件次數來概估。

(三) 脆弱點等級

是指個資檔案之脆弱點被威脅利用的容易程度。分級評等及分級原則如下表，進行分析時，符合分級原則欄中列出任一項者，即可視為該評等等級。

容易度	評等	分級原則	說明
高 (缺乏管控)	3	弱點很容易被利用 (例如：缺乏加密保護防護、缺乏有效管理病毒防護、實體環境未劃分安全區域出入管控) 。 尚未建立個人資料檔案保存、銷毀、監督程序，亦無實施任何管控措施。 缺乏相關管理防護及法規遵循機制。	符合左列任一條件即為 3
中 (管控不足)	2	弱點被利用的難度適中 (例如：已建立加密保護防護、病毒防護或劃分安全區域出入管控等防護機制但未落實) 。 已建立個資檔案保存、銷毀、監督程序，但未落實。 未建立個資檔案保存、銷毀、監督程序，但已實施部分管控措施。 相關管理防護及法規遵循機制不足。 已建立管理防護及法規遵循機制，但未落實。	符合左列任一條件即為 2
低 (管控已落實實施)	1	弱點很難被利用 (例如：已建立加密保護防護、病毒防護、劃分安全區域出入管控等防護機制並落實實施) 已建立個資檔案之保存、銷毀、監督程序，並落實實施。 已具備相關管理防護機制及遵法性機	符合左列任一條件即為 1

容易度	評等	分級原則	說明
		制並落實實施。	

七、 計算風險值與訂定風險等級

(一) 風險值之計算

風險值 =個資重要等級 * 脆弱點等級 * 威脅等級

(二) 訂定風險等級

將風險值組合可能的最大值與最小值相減，再分成四等級。即風險等級由最高至最低分別以 A、B、C、D 代表，風險等級所代表的意義說明於后：

等級	風險值落點	風險接受程度	說明
A	24、27、36	不可接受	最高風險值區間，此類風險發生可能嚴重違反個資法或嚴重未達良善管理之責，應及時進行風險處理。
B	16、18	不可接受	次高風險值區間，此類風險發生可能違反個資法或未達良善管理之責，應於考量人力與資源因素後，優先進行風險處理。
C	6、8、12	可接受	次低風險值區間，對個資法遵循性與資通安全影響不高，除遵循既有規定與透過現有安控措施進行管控外，尚需定期檢視風險值有無升高之趨勢。
D	3、4	可接受	最低風險值區間，對個資法遵循性與資通安全影響極小，遵循既有規定與透過現有安控措施進行管控即可。

八、 撰寫風險評鑑報告

各單位專人就執行前述各節內容所得的資訊與風險評鑑結果，送權責人員彙整撰寫風險評鑑報告(包括個資相關法規彙整表)後，交由本小組執行秘書，提報個人資料保護管理執行小組審閱。

九、 選定安控目標與機制

衡量個資相關法規命令、組織個資管理政策及個資安全控制措施規劃，建立組織相關個資管理安全控制措施，降低個資洩露或違反相關法規命令的風險。因預算、人力與資源可能有所限制，故應建立實施的優先順序，其選定的原則為「以可接受風險等級」為重點。

十、 撰寫與核准風險處理計畫

針對「不可接受之風險」與選定的安控目標與機制，評估經風險處理後之殘餘風險，使殘餘風險降低至可接受之風險程度內，然後將(1)不可接受之風險、(2)相對應之選定安控目標與機制及(3)評估後之殘餘風險，彙整後撰寫成風險處理計畫，提報至個人資料保護

管理執行小組審閱並核准實施。

陸、附錄

一、威脅/脆弱點相關資訊

	弱點	威脅	可能風險
1	未適當回應當事人對其個資之請求權	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
2	當事人通知停止處理利用或刪除時，缺乏停止處理與利用或刪除機制	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
3	委外管理之監督未落實(監督紀錄不全)	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
4	缺乏委外監督之資安要求	委外作業不當(不當存取，不當揭露，不當授權，不當利用等)	不符法令要求
5	個資項目有過度蒐集疑慮	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
6	蒐集當事人或非當事人個資未依法告知(優先關切非屬執行法定職務者)	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
7	主動刪除或停止處理(利用)個資程序不完備	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
8	個資更正或補充後，缺乏主動通知曾利用對象之機制	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
9	個資外洩時，缺乏主動通知當事人的機制	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
10	個資蒐集缺乏特定目的或有目的外利用情形	作業人員或使用者作業錯誤(不當)而違反個資法	不符法令要求
11	未依法公告於網站，並於建立個人資料檔案後一個月內為之，變更時亦同	作業人員或使用者作業錯誤(不當)而違反個法	不符法令要求
12	個資法相關教育訓練或認知不足。	作業人員或使用者作業錯誤(不當)而違反個資法	不當外洩或違反法令
13	有爭議或不清楚是否違反個資法	作業人員或使用者作業錯誤(不當)而違反個資法	違反法令
14	缺乏軌跡資料或不足	作業人員或使用者行	資料外洩無法舉證

	弱點	威脅	可能風險
		為不當(處理或利用或刪除或查詢)	
15	未適度遮罩(代碼或匿名或以星號取代)	個資遭不當揭露或利用	個資不當揭露
16	未遵循僅知(僅給予必要資料)或最小化原則(僅授權必要人員)	個資遭不當揭露或利用	個資不當存取
17	權限帳號設定不當	個資遭不當揭露或利用	個資不當存取
18	資料分級錯誤或處理不當(例如：含有個資之資料不當再生利用)	個資遭不當揭露或利用	個資外洩
19	處置(報廢或再利用)設備或儲存媒體時，未徹底刪除內含個資	個資遭不當揭露或利用	個資外洩
20	個資交換、傳輸或傳遞方式不安全	個資遭不當揭露或利用	個資外洩
21	資料保存不當(電子檔未加密／紙本未上鎖或存放地點實體安控不足/丟棄於資源回收箱)	遺失或遭竊取	個資外洩
22	儲存媒體處理或保存不當	遺失或遭竊取	個資外洩
23	未定期備份	毀損	影響業務運作
24	應用系統設計不當，在 AP 與 DB 伺服器之間以最高權限存取資料	竊取、竄改或洩漏	檔案遭不當存取或外洩
25	未定期弱掃或應用系統漏洞(例如 OWASP Top 10)未修補	竊取、竄改或洩漏	個資外洩
26	技術人員之安全程式撰寫能力不足	竊取、竄改或洩漏	個資外洩
27	權限帳號設定不當或未定期權限審查	竊取、竄改或洩漏	個資外洩
28	缺乏加解密規範與控管機制。(例如：資料庫缺乏加密或資料庫稽核機制)	竊取、竄改或洩漏	個資外洩