機密等級：內部文件

農業部
桃園區農業改良場

個人資料事件管理程序

第 1.0 版

113 年　8　月　22　日　　頒行

目錄

壹、目的

為保護本機關所保有的個人資料，防範個人資料被竊取、竄改、洩漏或不法等事件之發生，並維護機關聲譽，建立快速、有效、有秩序的個資事件管理程序，以便降低或排除個資事件所可能帶來的衝擊與傷害，強化個資事件處理能力，進而防範未來可能發生的個資事件。

貳、適用範圍

本管理程序適用於全場。

參、名詞定義

個資事件：任何疑似或確認個人資料被竊取、竄改、洩漏或不法等事件，致影響本場聲譽或有訴訟之虞。

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. 審核事件處理報告。
2. 審核與修訂個資保護管理制度文件。

(二) 本小組執行秘書

1. 分析歷年個資事件資訊，定期或不定期修訂個資保護管理制度文件。
2. 每年向本小組提報個資事件之統計分析報告及改善措施。

(三) 本小組委員

1. 瞭解個資事件原因與處理結果。
2. 負責個資侵害危機處理，必要時，得請求外力支援。
3. 於個資事件等級 1 與 2 級時，參考個資侵害危機處理小組執掌，協調相關單位組成團隊，因應後續危機處理。

(四) 兼辦政風

1. 對於涉及行政違失者，完成行政調查後，簽辦追究行政責任。
2. 對於不法個資事件涉有刑事責任者函送偵辦。

(五) 資安管理單位

1. 判定事件是否涉及電子資訊處理。
2. 若屬涉及電子資訊處理者，上網通報至行政院國家資通安全會報緊急應變中心。

(六) 各單位個人資料保護專責人員

1. 負責判定個資事件等級、影響範圍及所需資源。
2. 通報本小組委員、個資/資安管理單位、兼辦政風及相關權責單位。

3. 協助採取適當的管制措施。

4. 事件發生三十六小時內復原或完成損害管制，並於事件結束後回覆結案，填報「個人資料安全危害事件通報單」與「個人資料安全危害事件結案單」送交個資專責單位。

(七) 各單位保有個資業務承辦人

1. 評估個資事件處理所需時間，是否可能及時完成。

2. 依授權執行損害管制作業。

3. 負責執行個資事件應變與處理作業

4. 通知當事人個人資料受侵害項目、產生之影響及已採取之因應措施。

5. 對業務之範圍執行復原作業。

(八) 全體同仁

1. 瞭解個資事件之通報程序。

2. 對於已觀察到或懷疑可能發生的個資事件必須儘速通報各單位個人資料保護專責人員。

(九) 個資侵害危機處理小組

發生個資事件 3 級以上時，應成立個資侵害危機處理小組，進行應變處置，其職掌如下：

1. 總指揮(本場個資保護長)

(1) 授權副總指揮協調跨單位損害管制作業。

(2) 監控整體事件的發展。

(3) 督導各組運作。

(4) 主持會議。

(5) 審核新聞稿。

(6) 對外發言。

2. 副總指揮(各單位保有個資業務主管)

(1) 依授權跨單位協調損害管制作業。

(2) 協助總指揮處理相關事務。

(3) 事項安排、人力資源調配。

(4) 指導各組人員工作。

(5) 收集危機發生之人、事、物相關資料及物品。

(6) 審核個資事件原因與處理結果。

(7) 負責個資事件之任務管制與進度追蹤。

3. 農業推廣科

(1) 處理媒體採訪及安排記者會相關事宜。

(2) 協助發布新聞稿。

4. 兼辦政風

提供相關法律問題諮詢服務。

5. 應變處理組(個資保管單位)

(1) 通知有關支援單位。

(2) 對內通知危機處理相關人員。

(3) 準備對內、外說明之資訊。

(4) 保存、分析及提供相關之紀錄、存取軌跡等，負責查明事件發生之原因。

(5) 收集有關單位與事件報導的紀錄資料。

(6) 分析個資事件原因與處理結果。

(7) 準備危機事件處理報告。

6. 資訊組(資訊管理單位)

(1) 提供必要之諮詢與協助。

(2) 協助調閱防火牆與日誌伺服器等相關存取軌跡。

二、 執行時機

(一) 個資事件發生時。

(二) 欲透過演練以改善個資事件通報程序時。

三、 個資事件管理流程如附錄，詳細說明如下：

初期先將個資事件分為 4 個等級(詳如二、個資事件等級)以利判定，另可再考量下述「個資事件分析與判定」內容，予以調整事件等級：

(一) 個資事件分析與判定

1. 個資項目與其他資料結合之狀況

個資項目為判定事件等級之關鍵要素，若個資項目包括高風險個資，則事件等級應為 2 級以上；或個資項目為一般個資項目，但與其他資料對照、組合、連結後，事件等級可能從 1 級提升至 2 級。

2. 個資筆數

個資筆數之多寡不僅會影響受害之當事人，更會影響本場聲譽與處理該事件之人力、時間、處理方式及成本，例如若個資筆數很大，不僅需個別通知當事人還須公開說明事件處理經過與結果。

3. 個資被運用之難易度

個資是否容易被運用，是考量事件等級的要項之一。例如個資檔案沒有任何保護機制，用一般的工具就可以讀取並運用該資料，則事件等級就需提升；反之，若該個資檔案有經加密機制保護，則檔案被讀取之可能性低，則事件等級就可能降低。

4. 對本場或當事人之傷害程度

個資被有心人士運用，則有可能導致本場需支付最高賠償總額為新台幣二億元之巨額賠償金。若本場賠償金額或當事人財物損失愈高，則事件等級會較高。

5. 補救之難易度

判斷事件補救之難易度，有助於判定事件之等級。

(二) 個資事件等級

1. 『4』級：個人資料被竊取、竄改或洩漏且已遭不法利用，其數量達 30,001 筆以上。
2. 『3』級：個人資料被竊取、竄改或洩漏且已遭不法利用，其數量為 5,001 ~30,000 筆。
3. 『2』級：個人資料被竊取、竄改或洩漏且已遭不法利用，其數量在 5,000 筆以內。
4. 『1』級：個人資料被竊取、竄改或洩漏尚未遭不法利用。

(三) 個資事件通報

依前述肆、作業程序一、權責辦理。

(四) 個資事件處理方式

依據個資事件等級，判斷事件的處理方式：

1. 3 級與 4 級：依個資事件管理流程(八)個資侵害事件處理作業實施原則處理。
2. 1 級與 2 級：依本程序以及「矯正與持續改善程序」處理。若處理過程中，發現嚴重性比先前判斷的高而需提升等級時，則依實際等級之處理方式處理。

(五) 請求外力支援

當個資專人準備進行事件處理時，發現如下情況，可由本小組委員判定請求外力支援：

1. 人力不足。
2. 技術能力不足。
3. 專業能力不足。
4. 處理個資事件需使用的專業軟硬體設備不足。

可能的外力支援管道：

1. 專業個資或資安顧問。
2. 個資或資安設備與服務廠商。
3. 個資或資安相關專家學者。
4. 其他上級機關或政府機關個資或資安負責人員。

(六) 個資事件通報應變作業實施原則

1. 若於非工作時間發現個資事件，仍應依循程序通報。

2. 個資事件發生時，應盡量保持事件狀況，保全證據，以避免影響日後證據蒐集。
3. 提供事件所影響之資源與系統，供復原作業時參考。
4. 若需要資訊技術相關支援，應通知本小組委員協助，共同處理。

(七) 2 級以下個資事件處理作業實施原則

1. 識別事件所影響之資源與系統，供復原作業時參考。
2. 個資事件處理作業依照「矯正與持續改善程序」執行，並對個資事件受影響範圍依照「矯正-復原-檢討」的順序處理。
3. 處理作業內容應記錄備查，並經由權責人員審視確認。
4. 有關資訊技術方面，應依「資通安全事件管理程序」處理。

(八) 個資侵害事件處理作業實施原則

1. 成立個資侵害危機處理小組
   (1) 為將發生之個資事件危機控制在最小範圍，於收到通報後須儘速召集相關人員成立「個資侵害危機處理小組」。
   (2)「個資侵害危機處理小組」成員應共同瞭解與掌握危機發生原因及現況，研判危害程度與趨勢，決定妥善處理方式，隨時掌握發生狀況，進行因應。
2. 執行處理策略
   (1) 依個資侵害危機處理小組職掌，進行應變處置。
   (2) 有關資訊技術方面，應依「資通安全事件管理程序」處理。
   (3) 視情況,研擬對受害個資當事人可行的補救方案,例如賠償或其他替代方案。
3. 媒體溝通運作
   (1) 依據發生之事實，準備一切對內、外說明之資訊。
   (2) 處理媒體採訪及安排記者會事宜，由發言人對外發言。
4. 當事人相關之協調
   (1) 協調前，負責有關資訊、法令規章及專業意見等項目之諮詢準備。
   (2) 負責內、外部與當事人相關事務之通知。
   (3) 提供當事人進行後續申訴、仲裁、慰問、救助、賠償等程序之諮詢。
5. 善後與檢討

   檢討改進各單位對處理危機結果發現異常事項，依照「矯正與持續改善程序」執行，研擬矯正或持續改善措施，並確認該等措施之有效性。

(九) 個資事件彙總與分析

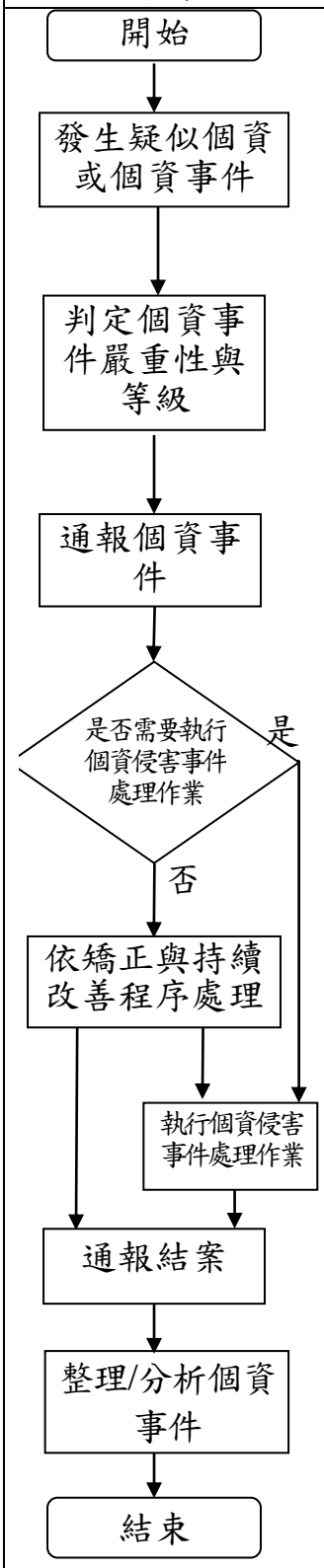
各單位個人資料保護專責人員收集並彙整個資事件，交由本小組執行秘書統計個資事件之數量、類別、等級、影響範圍、發生部門/系統等，並分析其中的異常變化，以便掌握矯正措施之有效性，發掘個資保護管理系統可能的脆弱點。常見的交叉分析類別如下：

1. 個資事件等級與數量。

2. 個資事件發生部門、系統、數量或平均等級。

伍、附錄

一、個資事件管理流程：

程序	說明
	● 當同仁已觀察到或懷疑可能發生的個資事件，或發生其他可能危害個資安全之現象時，應儘速通報各單位個人資料保護專責人員。 ● 各單位個人資料保護專責人員先判定是否為個資事件。 ● 各單位個人資料保護專責人員接著判定事件嚴重性、等級與影響範圍，以及釐清並告知範圍內保有個資之業務單位。若無法釐清權責單位，則應通報本小組。 ● 各單位依據事件嚴重性與等級，決定事件通報對象，並填寫「個人資料安全危害事件通報單」。 ● 各單位依據事件嚴重性與等級，決定事件的處理方式。 ● 各單位個人資料保護專責人員會同相關人員，依照「矯正與持續改善程序」進行事件處理。 ● 若發現事件等級需提升時，則執行個資侵害事件處理作業。 ● 依照個資侵害事件處理作業實施原則，進行緊急應變。 ● 事件發生三十六小時內復原或完成損害管制 ● 個資事件處理完畢後，填寫「個人資料安全危害事件結案單」，進行通報結案作業。 ● 各單位個人資料保護專責人員彙整個資事件處理紀錄，交予本小組執行秘書分析後，提報個人資料保護管理執行小組。

陸、參考文件

一、矯正與持續改善程序

二、資通安全事件管理程序

三、個人資料安全危害事件通報單

四、個人資料安全危害事件結案單