

個資事故通報處理及應變程序

一、 適用範圍

適用於所有與本校營運相關之個資事件及行為。本校人員及與本校成立契約關係或類似契約關係之第三人，包括但不限於供應商、承包商、約聘人員及顧問，如於執行本校相關業務時發生個資安全事故，皆應適用本程序。

二、 定義

(一) 個資安全事故

1. 個資發生被竊取、竄改、毀損、滅失、洩漏或其他侵害等事故。
2. 發生違反個資相關法令或本校個資保護相關規定之情形。
3. 其他涉及個資安全之事故。

三、 通報及應變程序

(一) 個資安全事故之通報程序

1. 於獲悉個資當事人抱怨、間接獲知個資因竊取、竄改、毀損、滅失、洩漏或其他侵害等，或是發現個資安全事故已發生或可能發生，應立即檢視事件重大性並於當日通報個人資料保護管理委員會（以下簡稱「個資委員會」）。
2. 倘事件具有緊急重大性，且涉及資訊設備之緊急修復時，同仁應於通報個資委員會後，迅速協助知會相關處理單位（例如：資圖處），進行處理。
3. 同仁於通報後，應即將通報內容及初步處理狀況記錄於「個資安全事故紀錄單」中，並送單位主管簽核後，由個資委員會保存。

(二) 個資安全事故之緊急處理程序

1. 個資委員會收到通報後，若認該事件將使個資可能在短時間內遭到毀損、滅失、洩漏或其他侵害時，或如不進行緊急處理可能使得損害快速擴大時，應即通知相關人員或協力廠商進行緊急處理。
2. 緊急處理措施
 - (1) 應以業管單位為原則，惟個資委員會視情況需要，得進行必要之指揮監督。
 - (2) 緊急處理時，應採取免於個資繼續受到毀損、滅失、洩漏之保護措施，例如於災難現場快速打包個資，並進行清點。
3. 緊急處理後，個資委員會應根據事故狀況進行調查、通報個資當事人、維護個資正確性、更正錯誤、改善整體環境或通報主管機關等作業。
4. 緊急處理後，個資委員會應將處理情形填載於「個資安全事故紀錄單」。
5. 關於事件發生後之個資正確性維護、錯誤之更正或整體環境之改善，由個資委員會責成相關單位進行後續處理。相關單位於後續處理完成後，應於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。
6. 如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知個資當事人及取得其書面同意。

(三) 個資安全事故處理程序

1. 於事故初步處理完畢後，個資委員會應依下列方式，查明事故發生之原因：
 - (1) 內部調查
 - A. 資訊單位：清查可能導致事故發生或資料外洩之缺口，透過檢視相關Log紀錄，如電子郵件傳送紀錄、資料下載紀錄等，分析可能導致事務之人員、時間及方式。

- B. 稽核單位：清查事故發生相關之作業程序，透過作業流程檢視、文件檢視、單位主管覆核紀錄等，以指出可能之問題所在。
- C. 各單位主管：檢視其單位之相關書面文件是否遭竊、非授權複製、拷貝等情況。

(2) 外部調查

- A. 得委託外部顧問本校進行鑑識稽核作業，透過特定檢視程序，對引起事故發生之可能處進行流程查訪，以確認問題之所在。
- B. 得委託徵信單位，對於本校內部可能導致事故之特定人員或外部有心人士進行可能犯罪行為進行收集、監視，並提供本校蒐集、分析之結果。
- C. 詢問個資當事人得知受害之相關情形和管道，並據以了解事件發生原因。
- D. 詢問導致事故發生之本校內、外部人員及其曾接觸之人員。

2. 查明事故發生原因後，個資委員會應填寫「個資安全事故通知當事人紀錄單」，並依照個人資料保護法第 12 條所要求，透過適當方式通知個資當事人，通知的內容應包括個資當事人個資被侵害之事實及本校已採取之因應措施，以及後續提供查詢及協助之方式。
3. 如符合相關法令需申報之規範，個資委員會另應依法向主管機關提出申報。
4. 事故發生後之個資正確性維護、錯誤之更正或整體環境之改善，由個資委員會責成相關單位進行討論及後續處理。相關單位於後續處理完成後，於「個資安全事故紀錄單」填載改善措施及從事故中學習到的經驗或課題。
5. 如因事故排除而有重新蒐集、處理及利用個資之必要，亦應重新告知當事人及取得其書面同意。

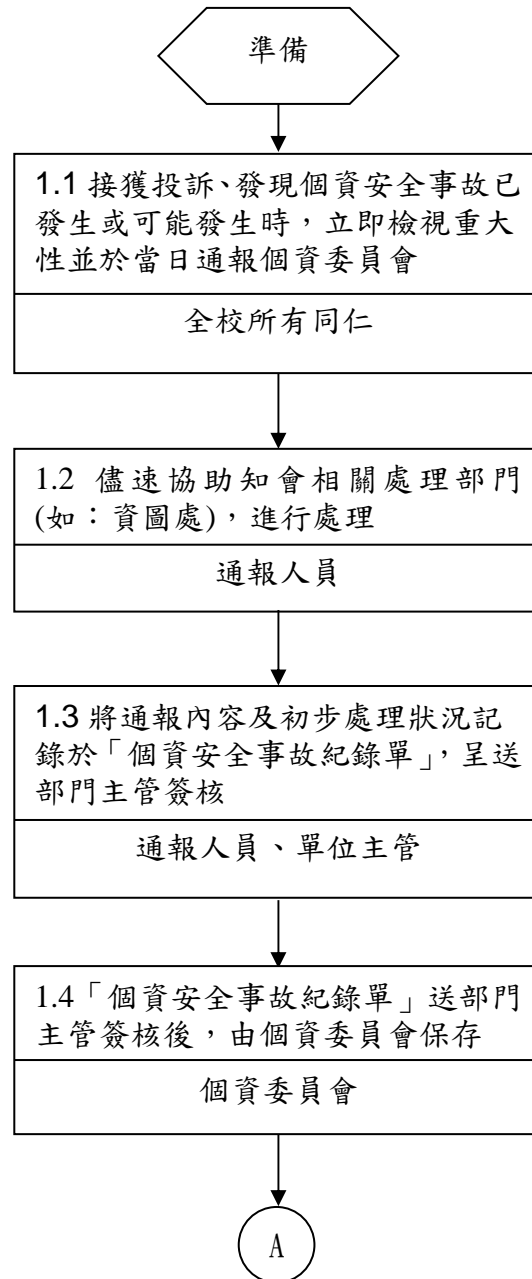
四、 獎懲原則

- (一) 員工如遵守本程序並通報個資安全事故，倘經個資委員會判斷該通報行為有效防止個資安全事故之發生或有效降低損害者，應給予適當之獎勵。
- (二) 員工如有隱瞞個資安全事故之行為，而致本校或負責人受有損害或有損害之虞，應給予警告或懲處。
- (三) 上述獎懲辦法由個資委員會訂定。

五、 稽核原則

個資安全事故之改善、預防措施及事故發生單位應列為內部稽核作業之重要查核範圍，並辦理追蹤考核。如發現不允當，應要求受查核單位立即改正，並報備個資委員會。

一、個資安全事故之通報程序



二、 個資安全事故之處理程序

