台北海洋科技大學個人資料檔案風險評估與管理程序書

104年10月27日104學年度第1學期第4次行政會議通過

104年11月16日海秘字第1040011240號令發布

106年7月24日105學年度第2學期第12次行政會議

106年9月18日海秘字第1060009396號令發布

一、 目的

台北海洋科技大學(以下簡稱本校)為個人資料檔案保護之風險管理制度，建立共同遵行之風險評估標準，規範高風險個人資料檔案之風險控制流程，以期有效降低個人資料檔案遭受損害之風險，特訂定本程序書。

二、 適用範圍

全校各單位。

三、權責劃分

(一) 個人資料保護管理執行小組

1. 風險評估結果審查。
2. 確認可接受風險程度。
3. 風險處理計畫審查。
4. 提供所需必要資源。

(二) 個人資料保護連絡窗口

1. 協助單位同仁進行個人資料檔案盤點與風險評估。
2. 彙整單位個人資料檔案清冊。

(三) 各單位

1. 個人資料檔案盤點
2. 個人資料檔案風險評估
3. 擬定並執行個人資料檔案風險處理計畫

四、名詞定義

(一) 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。本校個人資料檔案依存在之形式區分為系統資料、電子資料及紙本資料三大類。

(二) 系統資料

係指以應用系統存在之個人資料，並存放於伺服器資料庫中。

(三) 電子資料

係指儲存於硬碟、磁帶、光碟、隨身裝置等儲存媒介以數位形態存在之電子檔案。

(四) 紙本資料

係指以紙本形式存在之文書。

（五）可接受風險

係指對於個人資料檔案發生損害，本校可容忍的最大程度。

（六）剩餘風險

係指個人資料檔案於施行相關控制措施後所剩餘的風險。

五、作業說明

（一）個人資料盤點及風險評估執行時機本校每年定期執行一次個人資料盤點及風險評估作業。而於下列情形發生時，需再次對影響範圍內個人資料重新進行個人資料盤點及風險評估：

1. 學校組織、業務權責變更時。
2. 作業流程變更時。
3. 個人資料項目新增或異動時。
4. 發生重大資訊安全事件時。

（二）個人資料檔案盤點

1. 分析業務作業流程個人資料檔案盤點應由分析業務作業流程開始，由單位負責業務相關之程序與規範中（如：內部控制制度、標準作業程序、工作職掌、委外作業……等），了解資訊的流向。

2. 識別不同作業流程之個人資料項目

(1) 從業務或服務作業的流程中，分析各服務內容之作業流程與應用系統清單，以找出含個人資料之業務或服務作業流程，並找出與業務相關各種存在型式之個人資料檔案。

(2) 不同型式的資料，如書面紙本、電子檔案或備份資料等都應識別為不同的個人資料檔案。

3. 識別個人資料檔案的相關屬性識別出個人資料檔案的相關屬性，並填寫於個人資料盤點表中，相關屬性包含：

(1) 個人資料項目基本資料：特定目的、個人資料類別、檔案型態、權責單位。

(2) 個人資料項目生命週期活動：分析個人資料從蒐集、處理、利用、儲存、備份、傳輸、銷毀之活動及所需保存時間。

(3) 個人資料項目相關人員：當事人、內部單位、委外單位、供應者。

（三）建立個人資料檔案清冊

1. 個人資料盤點單位同仁依其所負責之業務，執行個人資料鑑別作業，填寫個人資料盤點表。

2. 個人資料專責人員應彙整單位內個人資料盤點表，建立「個人資料檔案清冊」。

（四）個人資料檔案風險評估

1. 各單位應確認單位對個人資料檔案保護是否落實。

2. 依據下列說明，對「個人資料檔案清冊」中所有個人資料檔案進行風險評估，並計算出每個個人資料檔案的風險值，並彙整於「個人資料檔案

風險評估彙整表」，提至個人資料保護管理執行小組會議報告。

(1) 個人資料價值評估(機敏等級)個人資料檔案的個人資料價值,依據每個檔案所含個人資料內容的機敏等級分別給予極高、高、中、低等四個不同之個人資料價值。但當個人資料檔案包含個人資料屬性越多，該個人資料的價值將會提升；相同的當個人資料筆數愈多，個人資料的價值亦會越高。

A. 機敏等級極高(權重值4):個人資料內容包含特種個人資料,如病歷、醫療、基因、性生活、健康檢查、犯罪前科、如種族、政治理念、宗教信仰、身心健康狀態(如諮商輔導紀錄)、性生活、犯罪記錄、訴訟相關記錄等。

B. 機敏等級高(權重值3):個人資料內容包含政府提供證號，如身分證號、護照號碼、稅籍編號等等，財務資訊如薪資、所得、資產、投資、負債、信用、銀行(信用卡)帳號、保單號碼、弱勢資訊、個人特徵詳細描述、敏感協商資料等。

C. 機敏等級中(權重值2):個人資料內容含有個人描述,(住址、電話、生日、身高體重、習慣等等)、家庭情形、社會情況、教育專長紀錄經歷、受雇情形等等資訊。

D. 機敏等級低(權重值1):個人資料內容只含姓名、學校產生的資料，如學生學號、班級、教職員職號、分機、職稱等等、公務聯絡資料(公司的名稱、電話、住址等等)。

(2) 衝擊程度評估當個人資料檔案發生外洩時,將可能對於個人資料當事人、學校本身及違反規定之人員造成不同衝擊，依其外洩可能的衝擊嚴重程度給予高、中、低等三個等級評估。

A. 衝擊構面一-對當事人損害程度

(a) 衝擊程度高(權重值3)：個人資料檔案資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。

(b) 衝擊程度中(權重值2)：個人資料檔案資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益嚴重受損。

(c) 衝擊程度低(權重值1)：個人資料檔案資料外洩對不致影響個人權益或僅導致個人權益輕微受損。

B. 衝擊構面二-對學校財務影響程度

(a) 衝擊程度高(權重值3)：所含個人資料檔案10000筆(含)以上。

(b) 衝擊程度中(權重值2):所含個人資料檔案200筆(含)以上，未滿10000筆。

(c) 衝擊程度低(權重值1)：所含個人資料檔案未滿200筆。

C. 衝擊構面三-對學校信譽形象程度

(a) 衝擊程度高(權重值3)：所含個人資料機敏等級與個人資料筆數

皆為高等，個人資料洩漏將非常嚴重影響學校形象與聲譽。

(b) 衝擊程度中(權重值2)：所含個人資料機敏等級高等(含)以上或個人資料筆數高等(含)以上，或個人資料機敏等級中等且個人資料筆數中等，個人資料洩漏將嚴重影響學校形象與聲譽。

(c) 衝擊程度低(權重值1)：所含個人資料機敏等級中等以下(含)或個人資料筆數中等(含)以下，個人資料洩漏將輕微損害學校形象與聲譽。

(3) 可能性評估學校制度管理的建置、執行與落實，影響個人資料檔案是否會個人資料外洩可能性，如人員的安全意識與專業技能、學校的作業管理規定與內部監督機制等，有良好的制度管理皆可降低事故發生的可能性，依其管理制度發展程度給予外洩發生的可能性高、中、低等三個等級評估。

A. 管理構面一-教育訓練

(a) 高風險(3)：

I. 業務相關人員未接受業務相關教育訓練，包含資訊安全個人資料保護認知、業務流程訓練、內控程序、職務專業訓練等。

II. 業務單位及學校並未有針對單位同仁任何教育訓練規劃，業務相關人員亦未能依需求提出教育訓練申請。

(b) 中風險(2)：

I. 業務相關人員只部分接受相關教育訓練，或接受訓練不完整，如資訊安全個人資料保護認知、業務流程訓練、內控程序、職務專業訓練等只接受部分訓練。

II. 單位有相關教育訓練規劃，但並未確實落實執行，業務相關人員只參加全校性教育訓練課程。

(c) 低風險(1)：

I. 業務相關人員有接受完整教育訓練，包含資訊安全個人資料保護認知、業務流程訓練、內控程序、職務專業訓練等訓練。

II. 單位有完整的教育訓練規劃，並確實落實教育訓練執行，業務相關人員能依規劃完成教育訓練課程。

B. 管理構面二-作業管理規定

(a) 高風險(3)：

I. 單位尚未建立與實施個人資料保護相關作業程序規範，業務同仁不了解個人資料保護該有的安全作業規定措施。

II. 該個人資料檔案之作業處理未訂有書面標準作業流程或程序，業務相關人員依自已處方式或經驗執行。

III. 單位有建立或實施個人資料保護相關作業程序規範，但並未確實落實，內部監督或稽核時有發現多樣缺失，已造成管理系統失效。

(b) 中風險(2)：

I. 單位有建立或實施個人資料保護相關作業程序規範，但部分並未確實落實，內部監督或稽核時有發現缺失。

II. 該個人資料檔案之處理流程部分訂有書面標準作業程序,但並未確實落實，內部監督或稽核時有發現缺失。

(c) 低風險(1)：

I. 單位已建立並實施個人資料保護相關作業程序規範。

II. 該個人資料檔案之處理流程皆訂有書面標準作業程序可以遵循。

C. 管理構面三-內部監督稽核

(a) 高風險(3)：學校或單位未建立內部稽核或監督管理機制，如內部控制、品質管理系統、資訊安全管理系統、個人資料管理系統。

(b) 中風險(2)：學校或單位有建立內部稽核或監督管理機制，如內部控制、品質管理系統、資訊安全管理系統、個人資料管理系統，但內部稽核或監督管理機制落實,單位並未每年執行稽核或監督審查。

(c) 低風險(1):單位已建立內部稽核或監督管理機制,如內部控制、品質管理系統、資訊安全管理系統、個人資料管理系統，單位落實每年執行稽核與監督審查，並確實執行持續改善。

D. 管理構面四-個人資料檔案不當存取

(a) 高風險(3):該個人資料檔案過去三年內曾發生超過一次以上 外洩或不當存取情形。

(b) 中風險(2)：該個人資料檔案過去三年內曾發生一次外洩或不當存取情形。

(c) 低風險(1)：該個人資料檔案過去三年內未曾發生過外洩或不當存取情形。

(d) 風險值計算依據個人資料價值、衝擊程度與可能性進行評估，所獲得之極高、高、中與低之評價，將其轉換成對應分數4、3、2與1分，以進行風險值計算。

I. 個人資料價值=機敏等級

II. 衝擊程度=Max(衝擊構面一，衝擊構面二，衝擊構面三)

III. 可能性=Max(管理構面一，管理構面二,管理構面三，管理構面四)

IV. 風險值=個人資料價值*衝擊程度*可能性

(五) 決定可接受風險之風險值

1. 依法令法規、客戶要求、合約、服務等級協議及營運需求等為基準，於個人資料保護管理執行小組中決定可接受風險程度之風險值。

2. 超過可接受風險程度之個人資料檔案，於會議中確認風險處理之權責單位。

（六）個人資料檔案風險處理

1. 風險處理權責單位，針對可能產生風險之威脅及脆弱點擬定安全控制措施提出「個人資料檔案風險處理計畫」，以期將風險降至可接受程度。

2. 各單位將「個人資料檔案風險處理計畫」提報個人資料保護管理執行小組審查，於會議中討論處理計畫內容並提供所需資源後，依計畫執行改善。

3. 個人資料保護管理執行小組應將「個人資料檔案風險處理計畫」列入追蹤管理，並定期確認其有校性。

4. 若個人資料風險處理計畫無法將風險降低至可接受範圍內，應評估其它安控措施或有效性量測方式，以確保個人資料檔案可受到完善之保護。

六、使用表單

（一）個人資料盤點表。

（二）個人資料檔案風險評估彙整表。

（三）個人資料檔案風險處理計畫。