大華科技大學

個人資料檔案風險評估與管理程序

機密等級：限閱

文件編號：B-005

版　　次：1.1

發行日期：104.05.19

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	103.05.27		蕭崇惠	初版
1.1	104.05.19		個人資料保護推動小組	修訂者修改為個人資料保護推動小組

個人資料檔案風險評估與管理程序					
文件編號	B-005	機密等級	限閱	版次	1.1

目　　錄

個人資料檔案風險評估與管理程序					
文件編號	B-005	機密等級	限閱	版次	1.1

一、目的：

為建立本校個人資料檔案之風險管理制度，提供共同遵行之風險評估標準，並規範高風險個資檔案之風險控制流程，特訂定本程序，以期有效降低個人資料檔案遭受損害之風險。

二、範圍：

本校各項涉及個人資料之業務所產生的個人資料均適用之。

三、權責：

會議/單位/人員	工作說明
風險評估審查會議	1. 風險評估結果審查 2. 確認可接受風險程度
風險處理計畫審查會議	1. 許可風險處理計畫 2. 提供所需必要資源
單位個資保護代表	1. 協助單位同仁進行個資檔案盤點與風險評估 2. 彙整單位個資檔案清冊
各單位	1. 個人資料檔案盤點 2. 個人資料檔案風險評估

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型態存在之電子案。

(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、作業內容：

(一).個人資料盤點及風險評估執行時機

1.本校每年定期執行一次個人資料盤點及風險評估作業

2.於下列情形發生時,需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).個人資料盤點

1.分析業務作業流程

個人資料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資項目

(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資檔案。

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、個資類別、檔案型態、權責單位。

(2). 個人資料項目生命週期活動：分析個資從蒐集、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. 單位個資保護代表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. 各單位應以「個人資料安全作業檢核表」確認單位對個人資料檔案保護是否落實。

2. 依據「個資風險評估填寫說明」,對「個人資料檔案清冊」中所有個資檔案進行風險評估，並計算出每個個資檔案的風險值，並彙整於「個人資料檔案風險評估彙整表」。

(五). 決定可接受風險之風險值

1. 於風險評估審查會議,協各業務單位依前項之彙整表內容提出「個人資料檔案風險評估報告」,並依法令法規、客戶要求、合約、服務等級協議及營運需求等為基準,於風險評估審查會議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資檔案,於會議中確認風險處理權責單位。

(六).個資檔案風險處理

1. 個人資料保護推動小組應協助風險處理權責單位提出「個人資料檔案風險處理計畫」，針對可能產生風險之威脅及弱點擬定安全控制措施，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」提報風險處理計畫審查會議審查，於會議中同意處理計畫內容並提供所需資源後，依計畫執行改善。
3. 個人資料保護推動小組應將「個人資料檔案風險處理計畫」列入追蹤管理，並定期確認其有效性。
4. 若個資風險處理計畫無法將風險降低至可接受範圍內,應評估其它安全控制措施或有效性量測方式,以確保個資檔案可受到完善之保護。

六、相關文件：

(一).個資風險評估。

七、使用表單：

(一).個人資料盤點表。

(二).個人資料檔案清冊。

(三).個人資料檔案風險評估彙整表。

(四).個人資料檔案風險評估報告。

(五).個人資料檔案風險處理計畫。