明志科技大學

個人資料檔案風險評鑑與管理程序書

出 版 者：明志科技大學 秘書室

文件編號：PS-02-004

機密等級：一般

使用本文件前，如對版本有疑問，請與文件維護員確認最新版次。

本文件歷次變更記錄：

版次	發行日	編撰者	說明	核准者
1.0	2016/10/18	李政其	個人資料檔案風險評鑑與管理程	黃植振
2.0	2017/06/26	簡璽恩	個人資料檔案風險評鑑與管理程	黃植振

目　　錄

1　目的.....3
2　適用範圍.....3
3　權責.....3
4　定義.....3
5　作業程序.....3
6　相關資料.....6

1 目的

為建立明志科技大學（以下簡稱本校）個人資料檔案風險評鑑與管理規範，提供共同遵行之風險評鑑標準，採取適當之對策或控制措施，以有效降低個人資料檔案遭受損害的風險，特訂定本程序書。

2 適用範圍

本程序書適用範圍為本校業務相關作業流程產生之個人資料檔案風險評鑑事宜。

3 權責

3.1 召集人：核定「校務業務清冊」、「個人資料檔案清冊」、「個資風險管理報告」及「風險改善計畫表」。

3.2 執行秘書：監督個人資料檔案風險評鑑之執行、覆核個人資料檔案風險評鑑報告、審查個人資料檔案風險處理計畫、審查及確認風險改善之有效性量測。

3.3 個資保護執行小組：訂定「風險類別參考表」、與各單位執行業務盤點與個人資料檔案鑑別作業、建議可接受風險等級，以及陳報「個資風險管理報告」。

3.4 業管單位：負責所屬單位業務範圍之風險評鑑作業。

4 定義：無。

5 作業程序

5.1 業務及個人資料檔案鑑別

5.1.1 各單位配合個資保護執行小組執行組織業務盤點作業，並定義各項業務名稱，視實際狀況進行內容調整，產生「學校業務清冊」。

5.1.2 依據「學校業務清冊」之作業流程分析結果，執行個人資料檔案鑑別作業，並將結果紀錄於「個人資料檔案清冊」。

5.1.3 本校除每年執行一次個人資料檔案鑑別作業外，於新增業務、業務內容或流程異動，針對變動範圍內的作業程序與個人資料檔案進行鑑別作業。

5.1.4 個人資料資產分類

5.1.4.1 紙本資料：係指以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、文件等紙本資料。

5.1.4.2 **電子檔案**：係指儲存於**使用者端**之硬碟、磁帶、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。

5.1.4.3 **校務資料庫**：係指儲存於電算中心資料庫之資料，例如學籍資料。

5.1.5 個資價值評估由個資機敏、個資數量(可能在財務面影響)、個資可識別性與個資欄位數(代表個資詳盡程度)、營運與聲譽面等構面所組成，評估公式如下，權重由當年度評估時討論決議之：

個人資料資產價值 =機敏等級*1.5＋ 數量等級*權重 1.5＋
營運與聲譽影響*1.5＋ 可識別等級 ＋ 欄位數量等級

評估值	機敏等級
4	個資檔案機敏等級極高，如個人資料保護法第 6 條所載之病歷、醫療、基因、性生活、健康檢查及犯罪前科，以及高敏感個資，

	如政治理念、身心健康狀態、輔導與諮商紀錄、訴訟相關記錄等
3	個資檔案機敏等級高，除了一般個資外，外加登載身分證號、護照號碼、財務資訊、弱勢資訊、個人特徵詳細描述、敏感協商資料等
2	個資檔案機敏等級中，個資內容含有個人描述(住址、電話、生日、身高體重、習慣等)、家庭情形、社會情況、教育專長紀錄、學經歷、受雇情形等資訊
1	資檔案機敏等級低，如姓名、學校提供之證號(學生證號、教職員證號)、職稱、分機等

評估值	個資數量
4	個資數量超過 1 萬筆，全數外洩或處理不當，造成財務影響可能達 2 億元以上
3	個資數量 5000~1 萬筆，全數外洩或處理不當，造成財務影響可能達 1 億元以上，2 億元以下
2	個資數量 1000~5000 筆，全數外洩或處理不當，造成財務影響可能達 1 千萬元以上，1 億元以下
1	個資數量 1000 筆以下，全數外洩或處理不當，造成財務影響可能達 1 千萬元以下

評估值	營運與聲譽面
4	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資會影響**核心業務**運作，導致機關形象、信譽受到嚴重損害
3	禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資會影響**部份業務(不含核心業務)**運作，導致機關形象、信譽受到損害
2	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資會影響**單項業務(不含核心業務)**運作，導致機關形象、信譽受到輕微損害
1	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資**不會影響業務**運作，機關形象、信譽不會受到損害

評估值	可識別性
4	可直接識別
3	可間接識別

2	不容易間接識別
1	無法識別

評估值	欄位數量
4	10 欄以上
3	6-9 欄位
2	3-5 欄位
1	2 個欄位以下

5.2 風險評鑑

5.2.1 個資保護執行小組應決定與本校有關且影響達成管理制度預期成果能力者之內、外部議題，以及依據已發生之資安事件、及潛在因素、歷史性數據、理論分析、經告知的意見與專家的意見及關注方之需求，進行資訊安全風險鑑別。

5.2.2 個資保護執行小組依據上述進行討論，產出學年度「風險類別參考表」作為風險評估參考依據。

5.2.3 業管單位依學年度「個人資料檔案清冊」及「風險類別參考表」進行風險評鑑，並將結果紀錄於「風險評估表」。

5.2.4 風險值計算方式為個人資料檔案之風險事件對各構面所產生之之影響：

綜合風險值 = 個人資料資產價值 x 各風險類別可能性

5.2.5 可能性由管理作為，以及風險類別發生可能性所構成，並分成四級，評估週期以學年為一週期為計算依據，定義如下表：

發生可能性	條件
4	學年期間發生過次數高於 3 次(含)
3	學年期間發生過次數 2 次
2	學年期間發生過次數 1 次
1	從未發生過

5.2.6 個資作業小組應衡量本校環境及作業之安全需求，對風險評估結果進行討論，與建議可接受風險等級與風險處理之優先順序，陳報召集人審核。

5.3 風險處理

5.3.1 風險處理方式可包含接受、降低、避免與轉移等。風險若超出可接受風險等級，應檢討控制措施之有效性，適時修正風險控管措施之執行辦法，記載於「風險改善計畫表」，並視需求修改「適用性聲明書」。上述「風險改善計畫表」及「適用性聲明書」需經會議審核。

5.3.2 「風險改善計畫表」內容須包含個資資產名稱、資產風險等級(值)、風險處理方式(或控制措施)、所需資源(如經費、教育訓練、設備、人力資源、環境或空間等)、負責部門與人員、預計完成日期、督導人員

5.3.3 執行秘書將風險評估結果、可接受風險等級及「風險改善計畫表」彙整成「個資風險管理報告」，陳報召集人核定。

5.4 覆核

5.4.1 執行秘書應對核定後之「個資風險管理報告」，進行控管與不定期陳報。

5.4.2 每年應至少執行1次風險評鑑，或當有系統新增、重大異動或作業環境改變時，可執行不定期評估。

6 相關資料

6.1 參考依據

ISO 31000 風險管理原則與指導綱要

資訊系統分級與資安防護基準作業規定

100 年度研考會個人資料保護參考指引(V1.0)

6.2 輸出文件

學校業務清冊

個人資料檔案清冊

風險類別參考表

風險評鑑表

個資風險改善計畫表

個資風險管理報告