# 大華科技大學

## 個資檔案風險評估

機密等級：限閱

文件編號：C-002

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 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| 個資檔案風險評估 | | | | | |
|---|---|---|---|---|---|
| 文件編號 | C-002 | 機密等級 | 限閱 | 版次 | 1.1 |

**目　　錄**

| 個資蒐集聲明 | | | | | |
|---|---|---|---|---|---|
| 文件編號 | C-002 | 機密等級 | 限閱 | 版次 | 1.1 |

一、 項目說明：

個資檔案風險評估分別評估下列幾個項目：

個資價值 – 為個資檔案所含包含之個資內值

衝擊程度 – 為當個資檔案發生外洩等事故時可能對個方面所產生的衝擊影響

可能性 – 該個資檔案發生如外洩等事故的可能性高低

由個資價值、衝擊程度與發生的可能性等三個因素決定個資檔案的風險值。

二、評估說明：

1. 個人資料檔案個資價值評估

個人資料檔案的個資價值，依據每個檔案所含個資內容的機敏等級分別給予低、中、高與極高等四個不同之個資價值。但當個資檔案包含個資屬性越多，該個資的價值將會提升；相同的當個資筆數愈多，個資的價值亦會越高。

| 個資價值 | 極高 | 高 | 中 | 低 |
|---|---|---|---|---|
| 機敏等級 | 個資檔案機敏等級極高，如個資法第 6 條特種個資與其他高敏感個資(如種族、政治理念、宗教信仰、身心健康狀態、性生活、犯罪 記錄、訴訟相關記錄)等 | 個資檔案機敏等級高，如身分證號、國籍、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 | 個資檔案機敏等級中,如個人、家庭、社會、教育、受雇資訊等 | 個資檔案機敏等級低，如姓名、學 校提供之證號、分機等 |

**(1).機敏等級極高：**

A.特種個資：指病歷、醫療、基因、性生活、健康檢查及犯罪前科等資料。

B.其他高敏感個資：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。

**(2).機敏等級高：**

以個資內容面看-個資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。

**(3).機敏等級中：**

以個資內容面看-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、教育專長紀錄經歷、受雇情形等等資訊。

**(4).機敏等級低：**

以個資內容面看-個資內容只含姓名、學校產生的資料(學生證號、教職員證號、分機、職稱等等、公務聯絡資料(公司的名稱、電話、住址等等)

2.個資檔案外洩衝擊評估

當個資檔案發生外洩時，將可能對於個資當事人、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低、中、 高等三個等級評估。

| 衝擊程度 | 高 | 中 | 低 |
|---|---|---|---|
| 對當事人損害程 度 | 個資檔案機敏等級高（含特種個資、特種身分、輔導紀錄等），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 | 個資檔案機敏等級中(含身分證號、財務資訊)，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 | 個資檔案機敏等級低,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 |
| 對學校財務影響程度 | 所含個資檔案 10000 筆(含)以上,若發生損害賠償對學校財務影響範圍非常大 | 個資檔案 200 筆(含)以下 10000 筆(含)以上，若發生損害賠償對學校財務影響範圍較大 | 個資檔案 200 筆(含)以下,若發生損害賠償對學校財務影響範圍較小 |
| 對學校形象影響<br>程度 | 若發生個資安全事故,將導致機關形象、信譽受到非常嚴重損害。 | 若發生個資安全事故,將導致機關形象、信譽受到嚴重損害。 | 若發生個資安全事故,將導致機關形象、信譽受到輕微損害。 |
| 對法律遵循影響程度 | 個資洩漏違反法令將可能造成最高兩年( 不含)以上徒刑 | 個資洩漏違反法令將可能造成最高兩年(含)以下徒刑 | 個資洩漏違反法令將可能造成拘役或罰緩處分 |

(1). 對當事人損害程度：

A. 衝擊程度高-

個資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-

個資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-

個資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。

(2). 對學校財務影響程度：

A.衝擊程度高-

以個資檔案筆數看-所含個資檔案 10000 筆(含)以上。

B.衝擊程度中-

以個資檔案筆數看-所含個資檔案 200 筆(含)以上 10000 筆以下

C.衝擊程度低-

以個資檔案筆數看-所含個資檔案 200 筆(含)以下

(3).對學校信譽形象程度：

A.衝擊程度高-

所含個資機敏等級高等(含)以上且個資筆數高等(含)以上,個資洩漏將非常嚴重影響學校形象與聲譽。

B.衝擊程度中-

所含個資機敏等級高等(含)以上或個資筆數高等(含)以上,或個資機敏等級中等且個資筆數中等,個資洩漏將嚴重影響學校形象與聲譽。

C.衝擊程度低-

所含個資機敏等級中等以下(含)或個資筆數中等(含)以下,個資洩漏將輕微損害學校形象與聲譽。

(4).對法律遵循影響程度：

A.衝擊程度高-

個資洩漏將違反相關法令規定,將可能造成最高兩年(不含)以上有期徒刑之刑事責任

B.衝擊程度中-

個資洩漏將違反相關法令規定,將可能造成最高兩年(含)以下有期徒刑之刑事責任。

C.衝擊程度低-

個資洩漏將違反相關法令規定，將可能造成拘役或科或併科罰金。

3.個資檔案外洩可能性評估

學校制度管理的建置、執行與落實，影響個資檔案是否會個資外洩 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低、中、高等三個等級評估。

| 可能性 | 高 | 中 | 低 |
|---|---|---|---|
| 教育訓練 | 1.業務相關人員未有接受相關教育訓練<br>2.單位並未有教育訓練的規劃 | 1.業務相關人部分接受相關教育訓練<br>2.單位有完整的教育訓練規劃，但並未確實落實執行 | 1.業務相關人接受完整教育訓練<br>2.單位有完整的教育訓練規劃，並確實落實教育訓練執行 |
| 作業管理規定 | 1.尚未建立與實施個資保護相關作業程序規範<br>2.該個資檔案之處理流程未訂有書面標準作業程序，依經驗共識執行。 | 1.已建立或實施個資保護相關作業程序規範，並未確實落實 2.該個資檔案之處理流程訂有書面標準作業程序，其餘依經驗執行，並未確實落實。 | 1.已建立並實施個資保護相關作業程序規範，並確實落實。 2.該個資檔案之處理流程皆訂有書面標準作業程序可以遵循。 |
| 內部監督稽核 | 單位未建立內部稽核或監督管理機制 | 單位有建立內部稽核或監督管理機制，但單位並未每年執行稽核 | 單位已建立內部稽核或監督管理機制，單位於每年執行稽核，並確實執行持續改善 |
| 個資檔案不當存取 | 個資檔案過去三年內曾發生一次以上外洩或不當存取情形 | 個資檔案過去三年內曾發生一次外洩或不當存取情形 | 個資檔案過去三年內未曾發生過外洩或不當存取情形 |

(1).管理構面一-教育訓練

A.高風險

業務相關人員未接受業務相關教育訓練,包含資訊安全個資保護認知、業務流程訓練、內控程序、職務專業訓練等。業務單位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

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，如資訊安全個資保護認知、業務流程訓練、內控程序、職務專業訓練等只接受部分訓練。

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

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

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。

(2).管理構面二-作業管理規定

A.高風險

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

該個資檔案之作業處理未訂有書面標準作業流程或程序,業務相關人員依自己處理方式或經驗執行。單位有建立或實施個資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

單位有建立或實施個資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。

該個資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

單位已建立並實施個資保護相關作業程序規範。

該個資檔案之處理流程皆訂有書面標準作業程序可以遵循。

(3). 管理構面三-內部監督稽核

A. 高風險

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、個資管理系統

B. 中風險

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、個資管理系統，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

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、個資管理系統，單位落實每年執行稽核與監督審查，並確實執行持續改善

(4). 管理構面四-個資檔案不當存取

A. 高風險

該個資檔案過去三年內曾發生一次以上外洩或不當存取情形

B. 中風險

該個資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

該個資檔案過去三年內未曾發生過外洩或不當存取情形

三、風險值計算

依據個資價值、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。

- 個資價值 = 機敏等級
- 衝擊程度 = MAX(衝擊構面 1，衝擊構面 2，衝擊構面 3，衝擊構面 4)
- 可能性 = MAX(管理構面 1，管理構面 2 ,管理構面 3，管理構面 4)
- 風險值 = 個資價值 * 衝擊程度 * 可能性

例如

| 個資價值 | 機敏等級 |
|---|---|
| 評定 | 中(2) |

| 衝擊程度 | 衝擊構面一 對當事人 | 衝擊構面一 對學校財務 | 衝擊構面一 對學校形象 | 衝擊構面一 對法律遵循 |
|---|---|---|---|---|
| 評定 | 中(2) | 中(2) | 高(3) | 中(2) |

| 可能性 | 管理構面一 教育訓練 | 管理構面二 作業管理規定 | 管理構面三 內部監督稽核 | 管理構面四 個資檔案不當存取 |
|---|---|---|---|---|
| 評定 | 低(1) | 中(2) | 低(1) | 低(1) |

個資價值 = 2

衝擊程度 = Max(2,2,3,2) = 3

可能性 = Max(1,2,1,1) = 2

風險值 = 2*3*2 = 12