國立交通大學個人資料檔案安全維護計畫

104 年 3 月 12 日 103 學年度第 1 次個人資料保護暨資訊安全推動委員會通過
104 年 7 月 2 日 103 學年度第 2 次個人資料保護暨資訊安全推動委員會修正通過

壹、 人員管理措施

一、處理個資檔案之人員職務如有異動，應將其所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置密碼外，應視需要更換使用者識別帳號。

二、個資存取權限之授權管理，視人員執掌角色所需，且以執行業務及職務所必要之最低資源存取授權為限，非專責處理特定個資者不得具有存取或查閱之權限，並留存使用者身分、識別帳號與其行為紀錄以供事後稽查。

三、處理個資檔案之人員，因業務上所擁有之個資負有保密義務，必要時可簽訂保密切結書，並確認於離職或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

貳、 作業管理措施

一、個資檔案應定期備份，並防止備份檔案被竊取、竄改、毀損、滅失或洩漏。

二、處理個資檔案相關之資訊系統或應用程式使用完畢後，應立即登出。

三、內部傳遞或與其他機關交換個資時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封，或對資料檔案壓縮加密，並對轉交或傳輸行為加以紀錄流向備查。

四、儲存個資檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個資檔案，以避免資料不當外洩，並採取下列銷毀措施：

（一）硬碟或隨身碟利用資料清除軟體或以物理方式破壞，清除資料內容。

（二）磁帶、光碟片、微縮片、積體電路晶片應以物理方式破壞，使其無法繼續使用。

五、含有個資之報廢紙張不得回收及再利用。

六、報廢之個資文件，紙本應用碎紙機或依其他核可之方式進行銷毀；電子檔案須確實刪除並清空資源回收筒。

七、可攜式儲存媒體之使用規範：

（一）可攜式儲存媒體如需連接本校電腦設備或網路時，應先進行病毒掃描。

（二）具機敏性之資料應避免長期存放於可攜式儲存媒體，如有儲存之必要時，應考量使用加密技術。

（三）非公務需求不得將載有機敏性資料之可攜式儲存媒體攜出辦公場所。

（四）可攜式儲存媒體如為機關內共同使用，使用者切記在使用完畢後將所有資料文件移除，以免資料遭他人誤用。

八、個資委外作業

（一）個資若委外建檔，應於委外合約中載明所處理之個資保密義務、資訊安全相關責任及違反之罰則。

（二）與委外廠商所簽訂正式書面協議或契約中，應明確陳述契約終止或解除時，相關個人資料之銷毀或交還程序。

參、物理環境措施

一、儲存個資之資訊設備應置於實體安全區域（如門禁控管之辦公區域或機房），或與外部網路隔絕（如防火牆），設置門禁、監視錄影及防火設備，避免有心人士或非授權人員存取。

二、儲存個資檔案之磁碟、磁帶及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如上鎖之保管箱、書櫃或檔案室），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

肆、技術管理措施

一、使用個人電腦、相關設備或系統處理個資檔案，應設置使用者登入帳號及密碼，帳號不得與他人共用，密碼則須符合安全之複雜度且定期更新。

二、儲存個資之資訊設備應安裝防毒軟體，並設定自動更新病毒碼及定期執行排程掃描。

三、儲存個資之資訊設備應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。

四、個資檔案禁止存放於網路芳鄰分享目錄，或設定存取權限至指定之目錄。

五、儲存個資之資訊設備應定期檢視、更新作業系統與應用程式漏洞。

伍、認知宣導及教育訓練

一、本校應對處理個資檔案之人員施予資訊安全與個資保護之教育訓練，並不定期宣導個資保護之重要性。

二、本校全體教職員生及相關經手個資之第三人應對個資保護法及其施行細則與相關管理規範有基礎認知。

陸、紀錄機制

各單位可依實際業務狀況及需求，針對下列個資處理相關活動進行紀錄之保存，以為未來舉證等用途：

一、個資交付、傳輸紀錄

（一）以 Email 方式，交付人應保留相關紀錄。

（二）系統提供授權人連線下載方式，系統應有連線紀錄可供查閱。

二、確認個資正確性及更正紀錄

（一）資訊系統設計應提供個人查閱本人之基本資料，並允許做適宜之資料更新，以維持個資正確性。

（二）當事人以其他方式(如電話、傳真、Email、信函等)請求更正時，處理人員除進行必要之身分查核程序外,尚應設法留存事件紀錄。

三、提供當事人行使權利紀錄

本校對外公開之網站中「提供當事人行使權利」應載明依據個人資料保護法第 3 條，當事人得行使之相關權利，例如請求閱覽等，並提供本校個資保護聯絡窗口之詳細資訊，例如聯絡人、聯絡電話、Email 及郵寄地址等。

四、工作人員權限新增、變動及刪除紀錄

承辦人員於職務異動時，資訊系統負責人應即對系統使用權限重新設定，並保留相關紀錄。

五、個資刪除、廢棄紀錄

執行個資盤點與風險評鑑時，個資保管人應對已超過保管期限之資料，列表紀錄後依規定銷毀及確認無誤，如碎紙與刪除電子檔案或依其他核可之方式進行銷毀。

六、教育訓練紀錄

（一）將取得授權之研習課程講義或簡報檔公告網站週知。

（二）應保留教育訓練紀錄。

柒、個人資料安全持續改善

一、個資風險評估

（一）個資檔案風險評估作業應每年進行。

1. 各單位應針對個人資料檔案清冊內容，建立風險評量之標準，包括影響及衝擊之程度與風險發生之機率。
2. 個資檔案之風險評估應依實際狀況，對照「影響及衝擊等級表」(表 1)及「風險發生可能性等級表」(表 2)內容，進行風險分析。

表 1 影響及衝擊等級表

	個資數量	敏感程度	影響程度
輕微(1)	50 筆以下	僅有一般識別資料，如姓名、服務單位、職稱、電子郵件地址等。	◎對本校形象無任何影響，資料外洩或遭竄改不致影響當事人權益，資料無須重新取得。 ◎該事件不會造成任何關於法令法規之影響。
嚴重(2)	◎一般個資 51~1,000筆	含有政府資料中之辨識者及財務資料等，如身分證統一編號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。	◎對本校形象造成輕微影響，造成的衝擊可接受；資料外洩或遭竄改對個人權益影響輕微，資料重新取得容易可立即回復。 ◎該事件造成承辦人遭受內部懲處或外部廠商違反訂定之契約 。
非常嚴重(3)	◎一般個資 1,001筆以上 ◎特種個資	含有特種個人資料。	◎對本校形象造成嚴重影響(媒體的負面報導)；資料外洩或遭竄改造成大規模個人權益損害，

	1筆以上		資料重新取得不易無法立即回復。 ◎該事件造成承辦人及其主管遭受懲處或嚴重違反法令規章。

表 2 風險發生可能性等級表

等級	評估標準
可能性低(1)	◎很少發生或無發生可能性 ◎5年期間沒有發生過
可能性中(2)	◎可能發生或偶爾發生 ◎1年內發生次數小於2次(或5年內發生次數小於10次)
可能性高(3)	◎經常發生 ◎1年內發生3次以上

3. 風險值計算

識別風險發生之可能性及影響衝擊程度，將此兩項評分相乘，即計算出該個資檔案之風險值(表 3)。

表 3 風險值

影響及衝擊等級表	風險發生可能性		
	可能性低(1)	可能性中(2)	可能性高(3)
非常嚴重(3)	中(3)	高(6)	高(9)
嚴重(2)	低(2)	中(4)	高(6)
輕微(1)	低(1)	低(2)	中(3)

二、內部稽核管理

（一）本校應建立內部稽核管理機制，以確保相關管理措施之有效性。

（二）本校應定期執行稽核作業，並針對缺失與潛在風險，規劃矯正及預防措施。

捌、本計畫經本校個人資料保護暨資訊安全推動委員會通過後實施，修正時亦同。