國立東華大學個人資料安全保護基本措施

103 年 12 月 3 日 103 學年度第 1 學期第 1 次資通安全暨個人資料保護宣導及執行小組通過
105 年 4 月 20 日 104 學年度第 2 學期第 1 次資通安全暨個人資料保護宣導及執行小組修訂通過

壹、人員管理

一、本校教職員工職務如有異動，其保管之個人資料（以下簡稱個資）檔案應列入移交，相關資訊系統存取權限應重新設定。

二、單位接觸個資檔案人員應依照本校個資政策要求，執行相關規定之程序，負擔個資保密義務，並於離職或合約終止時停用資訊系統使用者識別帳號，及繳回通行證及相關證件。

三、禁止使用 LINE、FB、Skype 或其他即時通訊軟體傳輸業務所知悉之個資。

四、禁止在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個資。

貳、作業管理

一、個資蒐集應秉持「適當、相當且不過度」，只蒐集必要個資，以降低個資外洩風險。

二、針對所保有之個資，部份甚為敏感的欄位內容，譬如：密碼、身分證號等，於蒐集、處理或利用時，加上適宜之遮蔽措施。

三、個資檔案使用完畢後，應立即退出應用程式。

四、個資檔案禁止存放網路共用目錄。

五、網路傳送個資檔案時，應對資料檔案加密，並再確認傳送對象無誤及請對方收到後回覆確認。

六、使用可攜式電腦儲存媒體時，遵循以下的使用規範：

1.確定電腦安裝之防毒程式及病毒碼都有定時更新，足以偵測隱藏之病毒後，方可去讀取可攜式電腦儲存媒體內的檔案。

2.暫存的個資檔案，使用後應確認刪除。

3.電腦使用應設登入密碼且符合密碼複雜難度要求。

七、影印、列印、傳真使用後須確認設備內並未遺留個資資料及原稿。

八、應定期備份含有個資電腦資料，及確認備份資料的可用性與安全性。

九、個人電腦報廢須對硬碟做低階格式化；移作他用時，應格式化硬碟後再重新安裝系統。

十、報廢之個資文件須用碎紙機銷毀；電子檔須確實刪除與清空資源回收桶。

十一、委託他人執行上述行為時，需對受委託人依個資法施行細則第八條規定為適當之監

督，並明確約定相關事項、方式、義務及責任。

參、物理環境管理

一、圖資中心主機房

1.為確保相關設施之安全，非權責單位指定之人員不得擅自進入或使用相關資訊設備。

2.若外部人員或未具進出權限之人員，因執行業務需求進入時，必須指派人員隨行並填寫「人員進出登記表」後方可進出，並遵守相關設備管理之規定。

3.機房之門禁紀錄，應適當保存與定期審閱。

二、校內各單位保有個資之辦公室、檔案室、電腦主機室

1.無人或下班最後一人離開時，需將辦公室關門上鎖。

2.下班時記得將敏感之文件與可攜式資訊設備存放於儲存櫃並上鎖。

3.辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

4.重要的辦公室、檔案室或電腦主機室應加裝監視器。

三、個人資料儲存媒體的保管

1.應對儲存媒體內重要的個資檔案加強安全管控，例如加密。

2.應有備份機制，以免重要資料遺失。

3.隨身碟只適宜儲存暫時性檔案，重要的個資檔案使用後應儘快刪除，以免因隨身碟遺失造成個資檔案外洩。

肆、技術管理

一、重要資訊系統主機應做防火牆設定。

二、重要資訊系統應適宜的限制存取 IP。

三、電腦作業系統及相關應用程式之漏洞，應常做修補。資訊系統主機必要時需定時做弱點掃描，讓主機維持在不易入侵狀態。

四、公務個人電腦應安裝防毒程式並設定自動更新病毒碼及 Windows Update。

五、存有個資的個人電腦及伺服器，應設定登入密碼，且其密碼要符合安全之複雜度，至少 6 碼以上，且定期需更換密碼一次。

六、個人電腦應設定螢幕保護密碼，且螢幕保護啟動時間定在 15 分鐘以內。

七、應維持個資存取權限的正確性，且原則上不得共用存取權限，並留意個資被存取的情

形。

八、於入侵偵防設備上，設定禁止人員使用點對點(P2P)軟體提供分享檔案。

九、每年執行個資盤點，檢查個資之使用狀況及存取情形。

伍、認知宣導及教育訓練

一、本校應鼓勵教職員工生參與校內外資訊安全與個資保護之教育訓練，並定期宣導個資保護之重要性。

二、每年本校校內至少舉辦 2 場(含)以上的個資保護相關宣導及教育訓練，以養成教職員工生個資保護的警覺性。

三、本校個資窗口負責單位應時常注意個資保護相關知識與訊息，並摘要彙整於「個人資料保護專區」網站，以作為教職員工生獲取個資保護資訊的重要管道。

陸、紀錄機制

一、個資交付、傳輸之紀錄

1.以 Email、人員傳遞方式，交付人應保留相關紀錄。

2.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、確認個人資料正確性及更正紀錄

1.資訊系統設計上應提供個人查核本人的基本資料，並允許做適宜之資料更新，以維持個資正確性。

2.個人以異於上述的其它方式請求更正時，如電話、Email、信函等，處理人員除做必要的查核身份程序外，尚應設法留存事件紀錄。

三、提供當事人行使權利之紀錄

本校「個人資料保護專區」網站中「提供當事人行使權利」應清楚說明，依據個人資料保護法第三條，當事人得行使之相關權利，例如(1)請求閱覽 (2)請求製給複製本 (3)請求補充或更正 (4)請求停止蒐集、處理或利用 (5)請求刪除，並提供本校個資窗口之詳細連絡資訊，例如連絡電話、Email及郵寄地址。

四、工作人員權限新增、變動及刪除紀錄

人員工作異動時，重要資訊系統負責人應即對系統使用權限重新做設定，並保留相關紀錄。

五、個人資料刪除、廢棄與移轉紀錄

執行個資盤點與風險評鑑時，個資保管人應對已超過保留期限的部份，列表記錄後依

規定銷毀及確認無誤，如碎紙、刪除電子檔與檔案移轉。個人資料業務終止後處理方法得參酌下列方式為之，並留存下列紀錄：

1. 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
2. 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
3. 其他刪除、停止處理或利用之方法、時間或地點。

六、教育訓練紀錄

1. 將取得授權之研習課程講義或簡報檔公告「個人資料保護專區」網站。
2. 應保留教育訓練舉辦紀錄。

七、因應事故發生所採取行為之紀錄

彙整之紀錄需妥善儲存與維護，以防潮溼或毀損；若不幸因天災導致紀錄模糊無法辨識或使用時，則應照相存檔，並收集天災相關紀錄報導，以茲證明。

八、存取個人資料系統之紀錄

為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，系統管理者應定時備份事件記錄檔；如有文件修訂之情形，應以文件修訂建議表紀錄，以備日後查詢。

九、備份及還原測試之紀錄

資料庫應為定時備份，應定期進行備份媒體復原測試。復原測試得選定任一系統或資料庫進行還原，測試備份系統、備份媒體、及復原程序的有效性，並填列「備份狀況紀錄表」。

十、所屬人員違反權限行為之紀錄

遇人員違反權限瀏覽、使用非職務所觸及之重要個資，視事件輕重緩急，進行通知改善、縮減使用權限、停止使用或其他必要之處置，並將該人員列入管理名單，以備日後查核。

十一、定期檢查處理個人資料之紀錄

每年執行個資盤點，檢查個資之使用狀況及存取情形，並於確認後更新檢查日期於日期欄位。

十二、計畫稽核及改善程序執行之紀錄

稽核人員於稽核時所發現之內部控制制度缺失、異常事項及其他缺失事項，應於年度稽核報告中據實揭露 ，並檢附工作底稿及相關資料，作成稽核報告，定期追蹤至

改善為止。

柒、本措施經資通安全暨個人資料保護宣導及執行小組通過，陳請校長核定後公布實施，修正時亦同。