南華大學個人資料安全保護基本措施

105年02月15日104學年度第1次資訊安全暨個人資料保護推行委員會議提案通過
105年3月7日104學年度第2學期第1次行政會議修訂通過
111年07月06日110學年度 資訊安全暨個人資料保護推行委員會議提案討論修正
111年7月25日110學年度第2學期第5次行政會議修訂通過

一、 南華大學（以下簡稱本校）依據『教育體系個人資料安全保護基本措施及作法』，針對本校個人資料安全保護之「人員管理措施」、「作業管理措施」、「物理環境管理措施」、「技術管理措施」、「認知宣導及教育訓練」與「紀錄機制」，訂立「南華大學個人資料安全保護基本措施」（以下簡稱本措施）。

二、人員管理措施

（一）本校各單位應設置「個資保護聯絡窗口」，協調聯繫個資事宜。

（二） 處理個資應採取權限區隔，非專責處理特定個資者不得具有存取或查閱個資之權限。

（三）處理個資檔案之人員，應簽訂保密切結書相關文件。

（四）處理個資檔案之人員職務異動時，應列冊移交相關儲存媒體及資料。

（五） 處理個資檔案之人員職務異動時，接替人員應於相關系統重置通行碼，並視需要更換使用者識別帳號

（六）處理個資檔案之人員離職或合約終止時，應取消或停用其使用者識別帳號。

三、作業管理措施

（一） 個人資料蒐集應秉持「適當、相關且不過度」以誠信、合法且適當之方式，並遵循相關法令，進行蒐集、利用或處理進行個資。

（二） 針對委外單位，應於契約上訂有明確的監督要求，且應定期執行監督並保留監督稽核紀錄。

（三） 使用可攜式儲存媒體前，應先進行電腦病毒掃瞄，確認無問題後始可使用。

（四） 交換紙本個資時，應採取彌封或其他具備保密機制之傳遞方式；交換含有個資之電子檔時，應對資料檔案加密或是透過加密通道、機制傳送。

（五） 針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。

（六） 儲存個人資料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人資料檔案，或以物理方式破壞之，以避免資料不當外洩。

（七） 個人資料銷毀處理時，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。

（八） 處理與個人資料檔案有關之資訊系統使用完畢後，應立即登出資訊系統。

（九） 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。

（十）學校、機構提供電子商務服務系統或個人資料保護法第六條所定個人資料種類之資通系統時，應採取下列資訊安全措施：

(1)使用者身分確認及保護機制。

(2)個人資料顯示之隱碼機制。

(3)網際網路傳輸之安全加密機制。

(4)應用系統於開發、上線、維護等各階段軟體驗證及確認程序。

(5)個人資料檔案與資料庫之存取控制及保護監控措施。

(6)防止外部網路入侵對策。

(7)非法或異常使用行為之監控及因應機制。

前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動；資通系統，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

（十一） 進行個人資料國際傳輸前，應檢視有無主管機關依個人資料保護法第二十一條規定為國際傳輸之限制，並且告知學生及教職員其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

(1) 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

(2) 當事人行使個人資料保護法第三條所定權利之相關事項。

四、物理環境管理措施

（一） 儲存個人資料之資訊設備或文件應置放於實體安全區域(如：門禁控管之辦公區域、機房）避免有心人士或非授權人員存取。

（二） 儲存個人資料之資訊設備或文件的實體安全區域，非權責單位人員或經授權同意人員不得擅自進入或使用相關資訊設備。

（三） 儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及防火設備，進入時應有專人隨行並記錄之，並遵守相關資訊安全管理之規定。

五、技術管理措施

（一） 處理個資檔案之個人電腦，應設置使用者帳號及通行碼，通行碼至少每六個

月更換一次，長度須為八位數(含)以上，且夾雜英、數或特殊符號。

（二） 電腦系統若有螢幕保護功能，必須設定啟用。啟用螢幕保護保護時間設定應小於 15 分鐘，且須設定繼續後以密碼保護功能。

（三） 重要資訊系統主機應啟用作業系統自建之防火牆設定，並依應用服務特性適宜的限制存取 IP，必要時需進行弱點掃描，並應適當進行弱點處理。

（四） 所有電腦必須安裝防毒軟體，不可任意關閉或移除且防毒軟體病毒碼須定期更新；電腦系統及應用軟體，須開啟自動更新功能或留意其更新資訊，以確保軟體的漏洞為已修補狀態。

（五） 具備存取權限之終端機不得安裝檔案分享軟體。

（六） 每年應進行個資盤點，檢查個資之使用狀況及存取情形。

六、認知宣導及教育訓練

（一） 本校應設置個人資料保護專區網站，提供個人資料保護法規、知識與訊息，以作為教職員工生獲取個資保護資訊的重要管道。

（二） 本校每年應進行個人資料保護法基礎教育宣導和訓練，使全校教職員工生知悉應遵守相關規定。

（三）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。

七、紀錄機制

（一）個人資料交付、傳輸之紀錄

(1) 交付個人資料時，應保留相關交付紀錄。

(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) 以電話、Email、信函等確認個人資料正確性，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） 個人資料當事人透過「南華大學個人資料權利行使作業程序」，申請查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用與刪除個人資料時，應留存事件紀錄。

（四）個人資料刪除廢棄紀錄

執行個資盤點與風險評鑑時，個資保管人應對已超過保留期限的部份，列表記錄後依規定銷毀及確認無誤，如碎紙與刪除電子檔。

（五）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。

（六）教育訓練紀錄

(1) 將授權之研習課程講義或簡報檔公告於本校「個人資料保護專區」。

(2) 應保留「認知宣導及教育訓練」之舉辦紀錄。

八、 本措施經本校資訊安全暨個人資料保護推行委員會及行政會議通過，陳請校長核可後公佈實施，修正時亦同。

南華大學個人資料保護管理制度檢核表

單　位			
填表人		填表日	年　　月　　日
E-mail		校內分機	

編 號	檢 核 項 目	符合	部分符合	未符合	不適用	未勾選「符合」者，請於本欄填寫原因
一、人員管理措施						
1	單位是否設置「個資保護聯絡窗口」，協調聯繫個資事宜？					
2	處理個資是否採取權限區隔，非專責處理特定個資者不得具有存取或查閱個資之權限？					
3	處理個資檔案之人員，是否簽訂保密切結書相關文件？					
4	處理個資檔案之人員職務異動時，是否列冊移交相關儲存媒體及資料？					
5	處理個資檔案之人員職務異動時，接替人員是否於相關系統重置通行碼，並視需要更換使用者識別帳號？					
6	處理個資檔案之人員離職或合約終止時，是否取消或停用其使用者識別帳號？					
二、作業管理措施						
1	單位是否遵循相關法令，進行蒐集、利用或處理進行個資？					
2	單位是否已針對委外單位，於契約上訂有明確的監督要求，且應定期執行監督並保留監督稽核紀錄？					
3	使用可攜式儲存前，是否先進行電腦病毒掃瞄，確認無問題後始可使用？					
4	交換紙本個資時，是否採取彌封或其他具備保密機制之傳遞方式；交換含有個資之電子檔時，是否對資料檔案加密或是透過加密通道、機制傳送？					
5	對有備份之個人資料檔，是否以適當方式保管？					
6	儲存個資檔案之電腦或相關設備如需報廢或移轉他用，是否刪除其內所儲存之個資檔案？					
7	個人資料銷毀處理時，文件是否用碎紙機銷毀，電子檔是否確實刪除與清空資源回收桶？					
8	處理與個人資料檔案有關之資訊系統使用完畢後，是否					

	登出資訊系統？						
9	是否已具備利用事務機器(例影印機、印表機或傳真機)列印、傳真或使用個資後，應立即取走之安全觀念？						
10	提供電子商務服務系統或個人資料保護法第六條所定個人資料總類之資通系統，是否有採取這 7 項資訊安全措施?	(1)使用者身分確認及保護機制					
		(2)個人資料顯示之隱碼機制					
		(3)網際網路運輸之安全加密機制					
		(4)應用系統於開發、上限、維護等各項軟體驗證及確認程序					
		(5)個人資料檔案與資料庫之存取控制及保護監控措施					
		(6)防止外部網路入侵對策					
		(7)非法或異常使用行為之監控及因應機制					
11	是否有國際傳輸個資資料?	(1)是否涉及國家重大利益					
		(2)國際條約或協定有特別規定					
		(3)接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞					
		(4)以迂迴方法向第三國（地區）傳輸個人資料規避本法					

三、物理環境管理措施						
1	儲存個資之資訊設備是否置放於實體安全的環境（如：具門禁控管、監視設備之辦公區域或機房）？					
2	儲存個資檔案之紙本或可攜式設備等相關儲存媒體，是否置於實體保護之環境？(例具門禁控管、監視設備之辦公區域、上鎖的櫃子)					
3	是否依據各業務屬性，指定人員負責管理儲存個資檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息？					
四、技術管理措施						
1	處理個資檔案之個人電腦，是否設置使用者帳號及通行碼？					
2	處理個資檔案之電腦或相關設備，是否設定電腦螢幕保護程式？					
3	重要資訊系統主機是否設定防火牆與限制存取 IP？					
4	公務個人電腦是否安裝防毒程式並設定自動更新病毒碼及 Windows Update？					

5	公務個人電腦是否杜絕安裝 P2P 分享軟體？					
6	是否每年完成個資盤點並建立清冊？					
五、認知宣導與教育訓練						
1	單位是否已清楚了解單位內有關個資之蒐集、處理、利用之範圍？					
2	單位若有蒐集特種個資，是否清楚了解單位內有關特種個資之用途？					
3	單位是否派員參加個資及資安相關教育課程？					
六、紀錄機制						
1	交換個資時，是否記錄轉交或傳輸行為之流向？					
2	在確認個人資料正確性時，是否留存確認紀錄？					
3	個人資料當事人申請查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用與刪除個人資料時，是否留存事件紀錄？					
4	單位是否有設計個資蒐集目的消失或屆滿之資料刪除程序？					

填表人　　單位主管