建國科技大學個人資料安全保護管理作業規範

中華民國105年11月23日行政會議初訂

一、建國科技大學（以下簡稱本校）依「個人資料保護法」(以下簡稱個資法)、「個人資料保護法施行細則」(以下簡稱個資法施行細則)、「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」及本校「建國科技大學個人資料保護管理辦法」等相關規定，實施本校個人資料安全保護管理作業內部稽核制度，特訂定本規範。

二、人員管理：

(一) 指定蒐集、處理及利用個人資料個別作業（以下簡稱個資作業）流程之所屬人員。

(二) 就個資作業設定所屬人員不同之權限，且定期確認權限內容設定之適當與必要性。

(三) 要求所屬人員遵守相關之保密義務。

三、作業管理：

(一) 運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，依循「電腦設備安全管理作業規範」。

(二) 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

(三) 個人作業過程有備份個人資料之需要時，比照原件，依個資法規定予以保護之。

(四) 個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等儲存媒體，俟該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該儲存媒體洩漏個人資料。

(五) 委託他人執行前款行為時，對受託人依個資法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。

(六) 當事人向本校請求補充、更正、刪除、停止蒐集、處理或利用個人資料者，應填具申請書並檢附相關證明文件，於三十日內為准駁決定，必要時得予延長至多三十日。

四、物理環境管理：

(一) 依個資作業內容之不同，實施必要之門禁管理。

(二) 妥善保管個人資料之儲存媒體。

五、技術管理：:

(一) 電腦設備或資訊系統上需設定認證機制，帳號及密碼具備一定安全之複雜度並定期更換密碼。

(二) 處理個人資料之電腦設備或資訊系統需安裝防毒軟體，並定期更新病毒碼。

(三) 對於電腦設備或資訊系統之作業系統及相關應用程式漏洞，定期安裝修補程式。

(四) 具備存取權限之電腦設備不得安裝檔案分享軟體。

(五) 定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。

六、認知宣導及教育訓練：

各單位應要求所屬人員參與個資法認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。

七、委外與自我檢核：

(一)委外進行個人資料之蒐集、處理及利用時須於契約中明確約定相關監督事項與方式，並要求受任人(廠商)填報檢核表，送交委任單位複檢。

(二)每年定期進行個人資料檔案盤點、風險評鑑及內部稽核。

八、紀錄機制：

為確認相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，應保存相關紀錄以供查驗。

(一)個人資料交付、傳輸之紀錄。

(二)確認個人資料正確性及更正之紀錄。

(三)提供當事人行使權利之紀錄。

(四)所屬人員權限新增、變動及刪除之紀錄。

(五)個人資料刪除、廢棄之紀錄。

(六)教育訓練之紀錄。

(七)個人資料檔案清冊與風險評鑑表。

(八)個資稽核結果報告書。

九、本規範經行政會議通過，陳請校長核定後公布施行，修正時亦同。