南臺科技大學個人資料安全管理實施辦法

民國104年6月22日行政會議通過
民國105年9月26日行政會議修正通過

第一章 總則

第一條　南臺科技大學(以下簡稱本校)為規範各單位個人資料管理作業，依據「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」及「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」，特訂定本辦法。

第二條　個人資料之管理目標需達到蒐集、處理、利用之合法性、安全性及當事人權益如下：

一、蒐集、處理、利用個人資料僅限於合法目的及公務用途。

二、尊重個資法保護資料當事人之權益。

三、保護個人資料安全。

四、賦予教職員工個人資料保護相關責任。

第三條　本校為落實個人資料保護與管理設置個人資料保護管理委員會，組織與責任另以「南臺科技大學個人資料保護管理要點」訂定之。

第四條　個人資料檔案風險管理機制，包括個人資料檔案清查、資料權責單位釐定、重要性評估、資料安全風險評估、適法性風險評估，依個人資料保護政策予以適當風險改善與建立管控措施。

第五條　所有個人資料的蒐集、處理須參照本辦法第二章「個人資料蒐集與處理」之規範。
個人資料保存與銷毀須參照本辦法第四章「個人資料檔案安全管理」之規範。

第六條　個人資料之提供與揭露須參照本辦法第三章「個人資料利用管理」之規範。

第七條　個人資料當事人依本辦法第五章「當事人權利管理」行使下述權利：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

第八條　各單位應遵守本辦法第六章「個人資料委外管理」之規範，以降低委託第三方蒐集、處理、利用個人資料所產生的資訊安全和違法風險。

第九條　有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料不得蒐集處理，但在徵得當事人書面同意或法令明定之情況下不在此限。

第十條　為加強教職員工有關個人資料保護之重要性的認知，學校相關單位須實行個人資料保護相關教育訓練。

第十一條 為落實本辦法之法令與規範的遵循，稽核室須依據本校內部控制制度之「個人資料保護管理作業」定期實施內部稽核與改善。

第二章 個人資料蒐集與處理

第十二條 直接蒐集與間接蒐集，應確認是否具備下列蒐集要件之一：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

第十三條 直接蒐集之法定應告知事項：

一、在蒐集個人資料時，必須告知當事人下列資訊：

(一)學校、機構名稱。

(二)蒐集之目的。

(三)個人資料之類別。

(四)個人資料利用之期間、地區、對象及方式。

(五)當事人依個資法第三條規定得行使之權利及方式。

(六)當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

二、有下列情形之一者，得免為前項之告知：

(一)依法律規定得免告知。

(二)個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(三)告知將妨害公務機關執行法定職務。

(四)告知將妨害公共利益。

(五)當事人明知應告知之內容。

(六)個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第十四條 間接蒐集個人資料時，必須向當事人告知個人資料來源及本辦法第十三條第一項第一款第一目至第五目所列事項。但符合個資法第九條第二項各款規定情形之一者，不在此限。前項之告知，得於首次對當事人為利用時併同為之。

第十五條 內部處理規定：

一、各單位每年依「南臺科技大學檔案分類及保存年限區分表」之規範檢視個人資料檔案留存是否符合規定。

二、本校跨單位之資料流通，應經權責單位審核並留存紀錄。

三、個人資料檔案應有適宜存取控管，避免未經授權之存取使用。

四、個人資料檔案的傳輸／國際傳輸，應考量其資料重要性採取適當安全的措施。

第十六條 資料共同管理與受託辦理活動之資料處理規定：

一、各單位確認個人資料與第三方機構共享乃依法律為之或雙方具有契約關係。

二、受託辦理活動之資料處理進行保護與保存須參照本辦法第四章「個人資料檔案安全管理」之規範。

第三章 個人資料利用管理

第十七條 個人資料利用之管理應遵循下列規範：

一、個人資料應在原蒐集目的範圍內或法定允許情況下利用。

二、超出原蒐集目的之利用由各單位確認其合法性。

三、資料利用應於達成目的之必要範圍內（最小揭露原則）為之。

第十八條 個人資料用於各種對外流通與推廣業務活動應遵循下列規範：

一、各單位確認本利用合於當初蒐集資料目的且於蒐集時已明確告知。

二、個人資料用於原蒐集特定目的外之利用，應符合個資法第二十條第一項規定始得開始利用。

三、當事人表示拒絕接受推廣時，應即停止利用其個人資料推廣。

四、首次推廣時，應提供當事人表示拒絕接受推廣之方式，並支付所需費用。

第十九條 本校承接外部委託業務活動若涉及個人資料之蒐集、處理、利用，應遵循下列規範：

一、若為受託活動之主辦單位，活動應告知當事人，資料之蒐集或將轉交委託單位。

二、若參與活動且非為主辦單位，應提醒委託單位/主辦單位告知當事人，資料將由本校協助處理。

三、受託活動所蒐集、處理、利用之個人資料不應超出該活動之使用範圍。

四、當認為委託單位之指示有違反個資法、其他個人資料保護法律或其法規命令時，應通知委託單位。

五、委託單位如有提出委外監督之條款，本校受託單位應遵守。

第二十條 第三方請求調閱個人資料應遵循下列規範：

一、本校配合資料調閱請求情況如下：

(一)司法、稅務、主管機關及其他依法律規定具有調查權之公務機關，因偵辦案件或行政管理需要調閱資料。

(二)非上述之其他機關請求提供資料，應敘明協助之事項及調閱範圍，行文本校並由各單位評估是否合於本辦法第十七條第一項第一款至第二款。

二、受理調閱資料案件時，為維護個人權益，各單位應確認調閱範圍及所依據之法令；除緊急情形外，應正式行文為之，否則不予受理。

三、所有資料調閱紀錄應由各單位自行留存。

四、調閱資料未獲核可者，受理調閱單位應註明不予提供資料之法令依據函覆調閱機關或第三方。

五、提供資料宜註明資料提供日。

第二十一條　將個人資料於公開易取得之途徑揭露時，應於達成目的之必要範圍內為之。

第四章 個人資料檔案安全管理

第二十二條　個人資料之管理應遵循下列規範：

一、個人資料檔案存取應建立可歸責性之帳號區隔或作業流程機制。

二、個人資料檔案之存取應與職責業務相關，未經授權不得存取與業務無關之個人資料。

三、敏感或大量個人資料之資訊處理設備或儲存設施，應有適當管控程序或區隔保護。

第二十三條　實體安全管理原則：

一、辦公環境無人監管時，存有個人資料之文件及可攜式儲存媒體必須上鎖保護。

二、公共使用之影印機、印表機、傳真機等之含有個人資料輸出，應儘快取回，避免遭他人誤用。

三、同仁應保持警覺，留意陌生人員進出辦公環境。

四、儲存敏感或大量個人資料之處所應具有門禁管理機制。

第二十四條　電腦安全管理原則：

一、電腦應維持作業系統修補更新，並評估必要的應用軟體更新。

二、電腦須安裝防毒軟體與即時更新病毒碼。

三、電腦應設定開機登入帳號密碼，密碼應至少包括大寫英文、小寫英文與數字，並且為8碼以上之長度。

四、電腦應設定15分鐘內啟動螢幕保護並以密碼鎖定。

五、筆記型電腦瀏覽器與本機郵件軟體禁止啟用密碼自動登入。

六、不宜將個人資料檔案留存於電腦桌面上；非作業需要，禁止將個人資料檔案儲存於分享資料夾。

七、點對點傳輸軟體依「南臺科技大學校園網路管理及流量管制要點」辦理。

第二十五條　可攜式儲存媒體管理原則：

一、可攜式儲存媒體儲存敏感或大量個人資料檔案時，應具開啟密碼保護機制。

二、可攜式儲存媒體應適當保管以避免遺失或遭竊。

第二十六條　資訊管理人員於系統管理時應遵循下列規範：

一、儲存個人資料之主機應設置防火牆保護。

二、儲存大量個人資料之主機提供網際網路服務時，應定期或於重大變更時進行弱點掃描。

三、主機應留存系統日誌。

四、重要系統之個人資料存取應留存應用系統日誌，例如個人資料更新、刪除等操作活動。

五、測試用資料應將個人資料欄位內容去識別化。

六、委外廠商進行系統開發、測試與維護時，未經資料權責單位許可，不得將個人資料檔案複製或攜出本校。

七、儲存敏感或大量個人資料之系統密碼檔案應加密儲存。

八、個人資料系統須定期進行備份，並確認備份資料之可用性。

第二十七條　教職員工職務交接作業應遵循下列規範：

一、人員離、調職，應遵循「南臺科技大學主管及承辦人員移交辦法」辦理；離、調職人員非經單位主管同意不得留存個人資料檔案複本。

二、離職人員之個人資料檔案歸還切結應納入離校手續。

第二十八條　刪除／移轉／銷毀作業應遵循下列規範：

一、紙本資料銷毀，應予以絞碎或其他無法還原之方式進行銷毀。

二、硬碟資料刪除／銷毀，須使用資料覆寫技術或實體破壞。

三、資料銷毀若委託外部單位執行，須確認其銷毀作業無法回復資料。

四、重要或大量之個人資料檔案業務終止時，應留存紀錄。

第二十九條　遇有個人資料檔案遭人惡意破壞毀損、作業不慎等安全事件，應進行緊急因應措施並留存紀錄及通報本校個人資料保護管理委員會。

第五章 當事人權利管理

第三十條　當事人依個資法第三條行使權利時應遵循下列規範：

一、個人資料權責單位應提供聯絡方式。

二、當事人請求作業應依本校相關文件程序辦理及酌收必要成本費用。

三、當事人請求與核對當事人身分之紀錄應留存，驗證身分之佐證資料於驗證後退還或銷毀。

第三十一條　拒絕請求應符合下列條件：

一、以下任一種情況請求查詢、提供閱覽或製給複製本，可免予提供資料：

(一)妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

(二)妨害公務機關執行法定職務。

(三)妨害該蒐集機關或第三人之重大利益。

二、當事人請求刪除、停止處理或利用該個人資料，因執行職務或業務所必須者，不在此限。執行職務或業務所必須之情形如下：

(一)有法令規定或契約約定之保存期限。

(二)有理由足認刪除將侵害當事人值得保護之利益。

(三)其他不能刪除之正當事由。

三、因法得拒絕當事人行使權利之情況時，應一併附理由通知當事人。

第六章 個人資料委外管理

第三十二條　委外作業應遵循下列規範：

一、受委託之外部單位的技術、組織應符合安全要求。

二、若為資料作業委外或技術作業委外，安全規劃應包括伺服器端、資料庫端、使用者介面與管理者介面等相關資訊安全要求。

三、若為管理作業委外或特殊業務及重要資料委外，安全規劃應包括：

(一)資料安全傳遞與保管等安全要求

(二)法律責任擔保

(三)切結書／合約簽訂

(四)事件通報機制

第三十三條　委外合約應遵循下列規範：

一、代表、受委託之外部單位提供個人資料處理服務時，應要求簽訂書面合約。

二、委外業務承辦人應確認受託委外廠商執行個人資料處理之狀況。

三、本校若為委託單位時，應遵守本辦法第二章「個人資料蒐集與處理」法定告知事項，並要求受委託單位以適當方式向當事人揭露本校提供之法定告知事項。

第三十四條　委託處理個人資料檔案之作業結束時，須確認個人資料歸還及銷毀並留存紀錄。

第七章 附則

第三十五條　本辦法如有未盡事宜，悉依個資法規定辦理。

第三十六條　本辦法經行政會議通過，陳請校長核定後公布施行，修正時亦同。