國立臺灣師範大學心理與教育測驗研究發展中心

資安及個資管理政策

文件編號：RCPET-G-A-001
機密等級：一般

版　　次：4.1

發行日期：111.10.10

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.03.11		NII	初版發行
2.0	103.10.31		NII-吳昭儀	依 ISO 27001:2013 要求，修訂本政策。
2.1	104.01.19	P.2、3	NII-吳昭儀	依 ISO 27001:2013 文件審查之發現事項，修訂本政策。
3.0	106.09.26	P.1、2	周紘正	修訂文件編號及版次，修改 2.2、3.3、5.3 之內容
4.0	109.10.01	All	DeKnow	資安及個資管理制度文件整併
4.1	111.10.10	P.2、3	個資執行組	調整段落、標點符號。

目　錄

1 目的

為確保國立臺灣師範大學心理與教育測驗研究發展中心（以下簡稱「本中心」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並為規範個人資料（以下簡稱個資）之蒐集、處理及利用，同時避免人格權受侵害，並促進個資之合理利用，特訂定資安及個資管理政策(以下簡稱本政策)。

2 適用範圍

2.1 資安管理適用範圍為本中心之全體人員、委外服務廠商、工讀生與訪客等。

2.2 個資管理適用於本中心及本中心業務往來之當事人、相關機關（構)、廠商及第三方機構，所涉及個資之蒐集、處理與利用等活動。

2.3 範圍訂定應考量：

2.3.1 背景環境、內外部議題。

2.3.2 關注方之要求事項（含法律、法規、合約)。

2.3.3 中心及其他單位所執行之活動間的界面及相依性。

2.3.4 相關驗證範圍及關注方所關注事項之鑑別結果，展現於驗證範圍核定函，並由召集人核定。

2.4 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本中心造成各種可能之風險及危害，各領域分述如下：

2.4.1 資訊安全政策。

2.4.2 資訊安全之組織。

2.4.3 人力資源安全。

2.4.4 資產管理。

2.4.5 存取控制。

2.4.6 密碼學。

2.4.7 實體及環境安全。

2.4.8 運作安全。

2.4.9 通訊安全。

2.4.10 系統獲取、開發及維護。

2.4.11 供應者關係。

2.4.12 資訊安全事故管理。

2.4.13 營運持續管理之資訊安全層面。

2.4.14 遵循性。

2.5 ISO 29151 個資隱私管理原則範疇涵蓋 12 項要點，分述如下：

2.5.1 使用及保護 PII 的一般政策。

2.5.2 同意及選擇。

2.5.3 目的適法性及規定。

2.5.4 蒐集限制。

2.5.5 資料極小化。

2.5.6 利用、持有及揭露限制。

2.5.7 準確性及品質。

2.5.8 公開、透明及告知。

2.5.9 個人參與及存取。

2.5.10 可歸責性。

2.5.11 資訊安全。

2.5.12 隱私遵循。

3 目標

為維護本中心資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全，期藉由本中心全體同仁共同努力以達成下列目標：

3.1 資安管理目標

3.1.1 確保本中心業務資訊需經權責單位授權才可存取，以維護其機密性。

3.1.2 確保本中心業務資訊之正確與完整，避免被竄改或損壞。

3.1.3 確保本中心資訊服務之持續運作，以維護資訊系統及其相關業務。

3.1.4 確保本中心各項業務之執行須符合相關法令或法規之要求。

3.2 個資管理目標

3.2.1 符合相關法令及主管機關規範之原則，建立完善之個資管理制度，確保業務範圍內個資均妥善管理。

3.2.2 業務範圍內有關個資之蒐集、處理及利用之作業流程，應防止個資遭受竊取、竄改、毀損、滅失、洩漏或其他不合理之利用，善盡善良管理人之注意責任，

以建立民眾信任基礎並維護當事人權益。

4 責任

4.1 本中心應成立資安及個資管理組織統籌資訊安全與個資管理事項推動。

4.2 管理階層應積極參與並支持資安及個資管理制度，並透過適當標準及程序實施本政策。

4.3 本中心全體人員、相關教育主管機關、各考區試務會、委外服務廠商及第三方、工讀生、臨時人員與訪客等，皆應遵守本政策。

4.4 本中心全體人員均有責任透過適當通報機制，通報資安及個資事件或弱點。

4.5 任何危及資安及個資之行為，將視情節輕重依本中心相關規定進行議處。

5 管理指標

5.1 為評量資安管理目標達成情形，特訂定資訊安全管理指標如下：

5.1.1 凡本中心機密業務資訊或考生個資，須達全年零外洩，以確保本中心相關業務之機密性。

5.1.2 凡本中心業務相關對外公開資訊之完整性，須達 100%，以確保本中心相關業務之完整性。

5.1.3 確保本中心資訊機房維運服務及關鍵業務系統服務之可用性達全年 98%以上。

5.1.4 為確保本中心資訊安全措施或規範符合現行法令、法規之要求，每年至少需執行兩次內部稽核，須達成 98%以上，以確保本中心相關業務之適法性。

5.2 本中心遵循個人資料保護法及其施行細則，並依實務作業執行以下事項：

5.2.1 涉及處理 PII 的組織應制定使用及保護 PII 的政策。

5.2.2 對於個資的蒐集、處理、利用，除合法及合於業務作業目的之外，嚴禁一切非法或非行政業務作業之行為；並公告予當事人相關告知事項及方式。

5.2.3 僅於業務執行行政作業過程中之特定目的內蒐集個資。

5.2.4 僅於法律規定及行政業務作業所須範圍蒐集最少之個資，並且不處理過多的個資。

5.2.5 僅針對特定目的，蒐集最少的個資，且不處理過多的個人資料。

5.2.6 利用、持有及揭露限制 PII 的處理以達到合法目的及預期目的。

5.2.7 確保 PII 處理的準確性，完整性，最新性，充分性及相關性以達到使用目的。

5.2.8 應提供明確之管道讓當事人知悉其個資將如何被使用及被誰使用的清楚資訊；本著合法、公平、公正、公開的合理處置原則，進行蒐集、處理、利用必要之個資，並建立管理制度，以合理且適切的處理所取得之個資。

5.2.9 為保持個資準確性，依作業性質及當事人之請求，予以保持最新；尊重當事人權利，建立相關處理流程，以達 PII 當事人參與及存取之目標。

5.2.10 應建立適當的安全維護措施（如：治理、隱私衝擊評鑑、承包者及 PII 處理者的隱私要求、隱私監控及稽核、PII 保護認知及訓練、PII 報告等），以達可歸責性之目標。

5.2.11 根據威脅風險評鑑或 PIA 的結果，PII 應受到適當控制措施措施的保護，以達資訊安全之目標。

5.2.12 嚴格遵守個資保護相關法規，包含其他法規豁免例外應用；並僅於合法及有適當保護的狀況下傳送個資至其他國家或地區，以達隱私遵循性之目標。

6 審查

6.1 本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本中心業務永續運作及個資保護之能力。

6.2 本中心召集人應每年至少審查乙次資訊安全及個資管理目標達成情形表，以確認資安及個資管理目標計畫之工作內容、所需資源、負責人員、達成時間及成果評估方式等資訊，以明確展現最高管理者對資訊安全之領導及承諾。

7 實施

本政策經本中心召集人核定後實施，修訂時亦同。