國立宜蘭大學

個人資料檔案安全維護計畫

機密等級：限閱

文件編號：NIU-PIMS-B-008

版　　次：1.0

發行日期：107 年 10 月 31 日

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	107 年 10 月 31 日		游佳欣	初版

目錄

個人資料檔案安全維護計畫					
文件編號	NIU-PIMS-B-008	機密等級	限閱	版次	1.0

1 目的

為確保國立宜蘭大學（以下簡稱本校）個人資料檔案管理之安全，並強化對個人資料之保護能力，防止個資外洩事件發生，達成持續改善之目標。

2 參考依據

2.1 「個人資料保護法」。

2.2 「教育體系資通安全暨個人資料管理規範」。

2.3 「國立宜蘭大學個人資料保護組織程序書」（NIU-PIMS-B-001）。

2.4 「國立宜蘭大學個人資料蒐集、處理、利用與安全管理程序書」（NIU-PIMS-B-004）。

2.5 「國立宜蘭大學個人資料稽核作業程序書」（NIU-PIMS-B-006）。

2.6 「國立宜蘭大學個人資料矯正預防管理程序書」（NIU-PIMS-B-007）。

3 適用範圍

本校承辦相關個人資料作業均適用。

4 權責

4.1 個人資料保護推動委員會（以下簡稱個保會）

4.1.1 個人資料保護管理政策之研擬與管理制度之審查。

4.1.2 個人資料保護事項權責分工之協調，並提供必要資源予以執行任務。

4.1.3 對所採用之技術、方法及程序之研議及評估。

4.1.4 個人資料保護相關事件之檢討及監督。

4.2 個資保護執行小組

4.2.1 協助各單位進行個人資料盤點與彙整。

4.2.2 各單位個人資料管理、保護及維護等事項，並落實於相關業務及人員。

4.2.3 負責規劃個人資訊管理制度之維運工作及文件之制／修定作業。

4.3 個資保護稽核小組

4.3.1 協助實施個人資訊管理制度內部稽核。

4.3.2 協助確認個人資訊管理制度實施之有效性，並鑑別潛在之風險。

4.3.3 協助追蹤矯正預防措施之處理與完成情形。

4.4 本校所有同仁

4.4.1 落實個人資料保護相關作業規範。

4.4.2 執行本校於各項個人資料保護之決策及交辦事項。

5 作業說明

5.1 個人資料管理安全

5.1.1 個人資料範圍包含自然人姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

5.1.2 本校應建立個人資料保護管理組織，並指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

5.1.3 本校應建立可再現性之風險識別方法機制，以鑑別組織處理相關個

人資料作業於個資生命週期過程中可能產生之風險，釐清並配合適當控制措施，降低風險於可接受範圍內。

5.1.4 本校對個人資料之蒐集、處理、利用、傳輸與銷毀應訂定相關管理規範，且符合適當、相關且不過度之使用原則，記錄個人資料之紙本文件或電子檔案，應妥善保管並建立存取管控機制，執行重點：

(1) 蒐集個人資料時應向當事人盡到告知義務，並取得同意。

(2) 個人資料之蒐集、處理與利用須評估目的及範圍為適當、相關且不過度，不處理無關或超過原來所陳述使用目的之個人資料。

(3) 處理個人資料之系統或業務，應每年定期檢視，確保個人資料處理之適當性及不過度使用。

(4) 個人資料存取權限之授權管理，必須依人員執掌角色所需，且以執行業務及職務所必要的最低資源存取授權為限。

(5) 含有個人資料之電子檔案或紙本文件，非日常作業之讀取、列印、存檔、交換、分享及銷毀等處理及利用行為，應提出申請，經核准後方可執行，以建立授權、監督及行為記錄機制。

5.2 事故預防、應變與通報機制

本校應提供單一窗口受理當事人之請求或申訴事件，及建立個人資料事故通報程序，確實記錄通報與處理情形，並追蹤應變措施之有效性，執行重點：

5.2.1 提供單一窗口受理當事人之請求，提供其個人資料之查詢、閱覽、

製給複製本。

5.2.2 當事人對本校處理個人資料不滿時，可透過電話或電子郵件方式提出申訴，並由專人受理。

5.2.3 建立完整之內部個人資料事故通報流程，於發生個資外洩事故時，必須告知當事人並留下通報與處理紀錄。

5.2.4 權責單位個資保護聯絡窗口應將相關異常通知、事故判斷及處理情形等相關資訊確實記錄，並陳報權責單位主管審核。

5.2.5 權責單位個資保護聯絡窗口於處理完成時，應確認應變措施之有效性，隨時回報權責主管及相關單位，並視情況調整應變措施。

5.3 個人資料保護

本校應確保個人資料受到妥善保護，避免非經授權之閱覽、存取，執行重點：

5.3.1 個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。

5.3.2 各單位公務文書及紙本郵件應有專人負責收發。

5.3.3 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖。

5.3.4 伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護。

5.3.5 個人資料檔案應建立保存期限，並確實辦理保存與銷毀。

5.4 內部稽核管理

本校應透過定期內部稽核管理，確認個人資訊管理制度與矯正預防措施之實施情形，執行重點：

5.4.1 建立內部稽核管理機制，確認個人資訊管理制度實施之有效性與落實情形。

5.4.2 每年至少辦理一次內部稽核，並針對控管結果之不符合事項與潛在風險，規劃改善及預防措施。執行改善及預防措施時，應完成以下事項：

(1) 確認不符合事項根本原因。

(2) 提出改善及預防措施。

(3) 紀錄執行結果。

5.5 實體環境與設備安全管理

本校應確保個人資料存放環境與設備之安全，避免未經授權之人員進出辦公環境，處理或儲存大量個人資料之資訊設備，應規劃安全防護程序，或採取適當隔離控管措施，執行重點：

5.5.1 本校同仁應保持警覺，留意陌生人員進出辦公環境，若發現身份不明或可疑的人員，應主動詢問其身份，並視需要通知駐警隊處理。

5.5.2 委外廠商及訪客應於本校各單位指定之區域內活動。

5.5.3 網路環境應建立安全防護機制，網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.5.4 存放個人資料之伺服器、應用系統及資料庫等必須啟用稽核日誌，以保存相關稽核日誌與軌跡資訊。

5.5.5 敏感性系統或處理大量個人資料之資訊設備，應採取適當控管程序或隔離措施。

5.6 人員管理及認知宣導教育訓練

本校應對組織內部人員規劃訓練課程，以提升人員個人資料保護之安全認知及警覺意識，並要求委外廠商人員遵循本校個人資料保護相關規定。

5.6.1 本校同仁、接觸個人資料之外部人員、委外服務廠商人員於在職及離、退職後，均不得洩漏所知悉之機敏資訊，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

5.6.2 權責單位每年應對組織內部人員規劃訓練課程，或派員參加外單位辦理之專業課程，以提升人員個人資料保護之安全認知及警覺意識。

5.6.3 委外廠商人員於專案服務期間所知悉之業務資訊，應遵守「個人資料保護法」及本校個人資訊管理制度相關規定，且不得對外透露。

5.7 安全控制措施有效性量測

個資保護執行小組依「個資法」、利害相關團體要求及個資管理制度需達成之重點項目及各單位個資保護作業項目可能發生風險，提列管理目標項目及訂定量測方法，彙整制訂「國立宜蘭大學個人資料管理制度有效性量測表」（NIU-PIMS-D-020），依其量測頻率，進行有效性評量，並將量測結果，於每年「個保會」提報並檢討，以作為下年度之目標量測標準項目。

5.8 個人資料安全持續改善

本校應建立個人資料管理持續改善機制，透過適當的矯正或預防措施，矯正因內部或外來威脅所產生之風險，以達成持續改善之目標，提升整體個人資料保護安全的強度。

6 相關表單

6.1 「國立宜蘭大學個人資料管理制度有效性量測表」(NIU-PIMS-D-020)。