國立宜蘭大學

個人資料保護組織程序書

機密等級：限閱

文件編號：NIU-PIMS-B-001

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

個人資料保護組織程序書					
文件編號	NIU-PIMS-B-001	機密等級	限閱	版次	1.0

1 目的

為有效推動與辦理國立宜蘭大學個人資料保護之各項工作，特成立個人資料保護組織，以擬定本校個人資料保護發展之方向、策略及步驟，進而使個人資料保護管理制度持續穩健的運作。

2 參考依據

2.1 「國立宜蘭大學個人資料保護推動委員會設置要點」

2.2 「國立宜蘭大學個人資料保護管理政策」（NIU-PIMS-A-001）

3 適用範圍

適用於全校。

4 權責

4.1 組織

本校個人資料保護推動事宜由個人資料保護推動委員會負責，該組織架構詳 5.1.1。

4.2 權責

負責本校個人資料保護之維護與落實，權責範圍包括下列各項：

4.2.1 本校個人資料保護政策之擬議。

4.2.2 本校個人資料管理制度之推展。

4.2.3 本校個人資料隱私風險之評估及管理。

4.2.4 本校個人資料保護意識提升及教育訓練計畫之擬議。

4.2.5 本校個人資料管理制度基礎設施之評估。

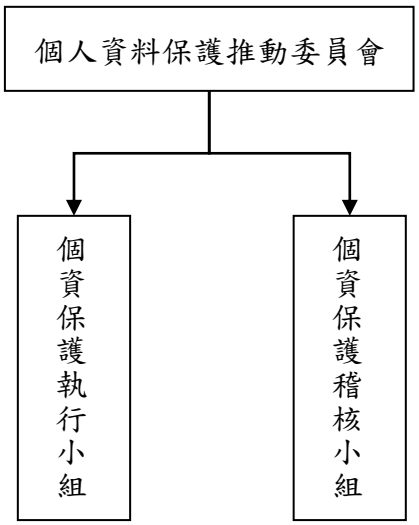
4.2.6　本校個人資料管理制度適法性與合宜性之檢視、審議及評估。

4.2.7　其他本校個人資料保護、稽核、管理之規畫及執行事項。

5　作業程序

5.1　組織

5.1.1　個人資料保護組織架構圖



5.1.2　設「個人資料保護推動委員會」，由校長指派一位副校長擔任召集人（個資保護長），另由圖書資訊館館長擔任執行秘書；本會委員依據「國立宜蘭大學個人資料保護推動委員會設置要點」委任，建立個人資料保護管理制度並推動個人資料保護相關事宜。

5.1.3　設「個資保護執行小組」,由一級行政單位及院級教學單位推派一人組成之，圖長資訊館館長擔任小組召集人，統籌各項個人資料保護作業原則規畫事宜。

5.1.4　設「個資保護稽核小組」，成員若干人由受過個資保護稽核訓練者組成，由個資保護長指派本校執行資安業務承辦單位主管擔任小

組召集人，負責個資保護稽核事宜。

5.2 建立個人資料保護組織全景

5.2.1 應依據個人資料保護推動委員會會議，與校內會議（如主管會報、行政會議或校務會議等）中有關個人資訊管理需求決議事項，或上級機關來文要求事項進行評估，並據此建立或調整個人資料管理範圍與目標。

5.2.2 應依據決議事項確認與該事項有關之利害相關團體與其要求，並留存文件化紀錄。

5.2.3 上述事項之識別與分析應每年至少審查一次，或於組織重大變更、新業務時重新檢視，並供管理審查時評估管理系統及其適用範圍調整必要性。

5.3 個人資料保護組織工作職掌

5.3.1 個人資料保護推動委員會

建立個人資料保護管理制度並推動個人資料保護相關事宜。

5.3.2 個資保護執行小組

(1) 依照個人資料保護推動委員會會議之決議，執行相關計畫。

(2) 建立個人資料保護管控措施監督機制。

(3) 檢討個人資料保護管理制度之變更管理、運作與成效。

(4) 規畫個人資料保護教育訓練及宣導事宜。

(5) 調查與處理重大個人資料保護事件。

(6) 於管理審查會議，提報個人資料保護管理系統執行績效與相關事項。

5.3.3 個資保護稽核小組

(1) 擬定稽核計畫。

(2) 執行稽核項目。

(3) 撰寫內部稽核報告。

(4) 針對稽核結果提出建議。

(5) 執行個人資料保護管理之內部稽核作業。

(6) 追蹤改善方案之執行成果。

5.4 保持與權責機關與特殊利害相關團體的聯繫

5.4.1 為確保個人資料保護事件發生時，儘速執行事件處理，須與權責或外部單位隨時保持聯繫，例如：主管機關、資通安全會報、消防單位等；並建立與組織個人資料保護管理制度相關之「個人資料保護外部單位聯絡清單」(NIU-PIMS-D-002)。

5.4.2 應隨時與個人資料保護技術相關團體維持聯繫，獲取個人資料保護技術及產品資訊與知識，以及處理個人資料保護事件或執行系統修補資訊等。並將資訊建立於「個人資料保護外部單位聯絡清單」(NIU-PIMS-D-002)。

5.5 個人資料保護目標的達成計畫與量測方式

5.5.1 個人資料保護目標應與個人資料保護政策一致並可量測，同時應

考量適用之個人資料保護要求，以及風險評鑑及處理之結果。並將個人資料保護目標與相關事項傳達給本校人員、委外廠商與個人資料作業相關單位，且於定期或組之重大變更時進行更新。

5.5.2 應定期規畫達成個人資料保護目標作業，並詳列於「國立宜蘭大學個人資料管理制度有效性量測表」(NIU-PIMS-D-020)，由個資保護執行小組負責維護更新。

5.6 提供資源

依據「國立宜蘭大學個人資料管理制度有效性量測表」(NIU-PIMS-D-020)與管理審查會議之決議適當分配資源。

5.7 維持組織內人員個人資料保護能力與認知

5.7.1 人員個人資料保護教育訓練

5.7.2 依所需職務之角色及業務內容，指派受過適當教育訓練、具備證照或具有經驗人員，執行個人資料保護管理相關任務。

5.7.3 如進行個人資料保護教育訓練則可安排以下類別訓練，例：

5.7.4 個人資料保護管理/技術課程。

5.7.5 個人資料保護稽核訓練課程。

5.7.6 主管個人資料保護課程。

5.7.7 規畫培訓以強化人員能力時，應對人員進行評估以確認培訓之有效性。

5.7.8 應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員

勝任之證據。

5.7.9 個人資料保護宣導

組織可利用內部網路系統（Intranet）、廣播、海報...等方式，隨時對組織員工公告個人資料保護威脅、個人資料保護新聞、病毒最新情況與相關因應方式，以提升員工個人資料保護意識。

5.8 運作之規畫及控制

5.8.1 各單位應依據管理制度各階文件的相關個人資料保護程序與管控措施，以及「國立宜蘭大學個人資料管理制度有效性量測表」（NIU-PIMS-D-020）與「國立宜蘭大學個人資料檔案風險處理計畫」（NIU-PIMS-D-009）內相關執行措施，進行個人資料保護作業並應保存保存執行證據。

5.9 監督、量測、分析及評估

5.9.1 個資保護執行小組依據「國立宜蘭大學個人資料管理制度有效性量測表」（NIU-PIMS-D-020），定期進行監督與量測，並以該量測結果做為評估本校個人資料保護目標達成情形。

5.9.2 應每年檢視「國立宜蘭大學個人資料管理制度有效性量測表」（NIU-PIMS-D-020）之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

5.10 個人資料保護獨立審查—管理審查

5.10.1 應定期（每一年至少執行一次）召開管理審查會議，並將報告與

決議事項於個人資料保護推動委員會進行報告（可配合組織內之主管會議同時進行）。

5.10.2 管理審查決議事項應能提供 PIMS 的潛在變更之詳細資訊，例如，識別政策、可能影響遵循性之程序與技術等調整內容。

5.11 個人資料保護管理系統持續改善

個人資料保護管理系統應持續改善管理制度的合宜性、適切性及有效性。

5.12 組織紀錄的保護

紀錄依紀錄型式（例如：變更紀錄、資料庫紀錄、錯誤日誌、稽核日誌和運作程序）進行分類，訂定保存期間和儲存媒體型式（例如：紙張、磁片、磁帶、硬碟或光碟片等儲存媒體）。並應依據資訊等級進行適當地處置與保護。

6 相關表單

6.1 「國立宜蘭大學個人資料保護外部單位聯絡清單」（NIU-PIMS-D-002）

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

6.3 「國立宜蘭大學個人資料檔案風險處理計畫」（NIU-PIMS-D-009）