

國立宜蘭大學

個人資料蒐集、處理、利用與安全管理程序書

機密等級：限閱

文件編號：NIU-PIMS-B-004

版 次：1.2

發行日期：110 年 12 月 01 日

個人資料蒐集、處理、利用與安全管理程序書

文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2
------	----------------	------	----	----	-----

目錄

1	目的	1
2	參考依據	1
3	適用範圍	1
4	權責	1
5	定義	1
6	作業說明	2
7	相關表單	12

個人資料蒐集、處理、利用與安全管理程序書				
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次
				1.2

1 目的

國立宜蘭大學（以下簡稱本校）為落實辦理「個人資料保護法」（以下稱個資法）規定之個人資料蒐集、處理、利用與安全，特訂定本程序書。

2 參考依據

2.1 「個人資料保護法」。

2.2 「國立宜蘭大學個人資料文件管理程序書」（NIU-PIMS-B-002）。

2.3 「國立宜蘭大學個人資料風險評鑑與管理程序書」（NIU-PIMS-B-003）。

3 適用範圍

本校所有同仁及相關委外合作廠商，所產生或經手之書面、電子個人資料均適用之。

4 權責

由個人資料保護推動委員會指派專責單位擔任本校個人資料連絡窗口，主要負責辦理下列事項：

4.1 個人資料抱怨、申訴與外洩事件之連絡窗口。

4.2 個人資料保護業務之協調聯繫及緊急應變通報。

4.3 彙整個人資料檔案安全事件之通報。

5 定義

5.1 個人資料

泛指自然人之姓名、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、

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

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。

5.2 蒐集

係指以任何方式取得個人資料。

5.3 處理

係指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

5.4 利用

係指將蒐集之個人資料為處理以外之使用。

5.5 當事人

係指個人資料之本人。

5.6 儲存媒體

如磁片、磁碟、磁帶、IC卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

5.7 國際傳輸

指將個人資料作跨國（境）之處理或利用。

6 作業說明

6.1 個人資料之蒐集控管原則

6.1.1 各單位使用個人資料需依「個資法」之特定目的必要範圍內為之，如為法定職務外、或特定目的以外之利用時，應向當事人履行告知

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

義務，並依據「個資法」規定，請當事人填寫「國立宜蘭大學個人資料提供同意書」(NIU-PIMS-D-010)取得當事人書面同意，或與當事人有契約或類似契約之關係。

6.1.2 本校相關活動之「國立宜蘭大學個人資料提供同意書」

(NIU-PIMS-D-010)及「國立宜蘭大學隱私權政策聲明」

(NIU-PIMS-D-014)，經該單位主管審核。

6.1.3 各單位蒐集個人資料時，應明確告知當事人以下事項：

(1) 本校名稱、聯繫方式。

(2) 蒐集目的。

(3) 個人資料的類別。

(4) 向當事人說明資料使用期間、保存期限、使用範圍及使用方式。

6.1.4 當事人可以行使之權利及方式，例如當事人可請求查詢、閱覽、製給複製本、補充、更正、刪除、停止蒐集、處理或利用。

6.1.5 向當事人說明可自行判斷是否提供個人資料，若為本校提供服務時所必須之資訊，因而造成無法提供該服務情形時，讓當事人瞭解對其個人權益之影響。

6.1.6 本校蒐集之個人資料若使用於行銷目的，應明確告知當事人拒絕接受行銷之方式（例如提供免付費電話、或免費回郵信封等）。

6.1.7 本校如於網站上蒐集個人資料時，應說明採用之技術收集並儲存資訊之方式，如 cookies 等。

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

6.1.8 上述程序所留存之必要的紀錄如:告知事項與當事人書面同意之紀錄，應等同或超過個人資料留存之時間，並維持內容之完整。

6.1.9 各單位於蒐集個人資料檔案時應注意下列事項：

6.1.9.1 評估蒐集目的及範圍為適當、相關且不過度，不處理無關或超過蒐集目的之額外的個人資料。評估蒐集目的及範圍程序如下：

- (1) 各單位因業務需求蒐集個人資料前，應先確認蒐集個人資料之目的與範圍。
- (2) 應確保特定目的所蒐集之個人資料不會用於其他目的，除非符合個人資料保護法第十六條或第二十條第一項特定目的外利用要件。
- (3) 承上，若將個人資料用於新特定目的，須取得當事人之自由意識下表示之書面同意。
- (4) 各單位定期透過內部稽核方式檢視蒐集之個人資料不逾越其目的。

6.1.9.2 處理未成年人相關個人資料時，應取得法定監護人的同意。

6.1.9.3 各單位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。

6.1.9.4 經由不同來源或特定目的取得的個人資料，進行比對而產出的個人資料，其使用亦應符合特定目的或遵循相關法律要求。

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

6.1.9.5 各單位間接蒐集非由當事人提供之個人資料時，應於處理或利用前，確認是否已取得當事人同意且已向當事人告知個人資料來源、本校名稱、蒐集之目的、個人資料之類別、個人資料利用之期間、地區、對象及方式、當事人依「個資法」第三條規定得行使之權利及方式。

6.1.9.6 各單位應依「個資法」第 17 條規定，每年定期審閱單位保有之個人資料，公開於本校指定網頁或其他公開管道。

6.2 個人資料之處理控管原則

6.2.1 處理個人資料檔案之個人電腦，應設置使用者登入帳號及密碼，並啟動螢幕保護程式密碼功能，相關存取原則依據「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001) 辦理。

6.2.2 應避免開啟個人網路分享目錄與檔案，或設定存取權限至指定之目錄。

6.2.3 本校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。

6.2.4 本校同仁若因業務需求，使用儲存媒體存放個人資料檔案時，應依「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001) 辦理。

6.2.5 處理個人資料檔案之本校同仁，應依「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001) 辦理；委外廠商應依「國立

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001)訂定合約辦理之。

- 6.2.6 維護人員或系統服務廠商遠端存取原則依據「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001)辦理。
- 6.2.7 處理個人資料檔案之人員職務異動時，應依據「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001)辦理。
- 6.2.8 處理個人資料檔案之應用系統，應將個人資料檔案的安全需求納入系統開發考量。
- 6.2.9 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，程序如下：
- 6.2.9.1 權責單位主管應確認個人資料存取之所需最低權限，並定期審核。
- 6.2.9.2 權責單位主管應定期審核人員之個人資料存取作業是否於合法目的下執行。
- 6.2.10 使用者存取權限管理依據本校「國立宜蘭大學個人資料安全控管作業說明書」(NIU-PIMS-C-001)辦理。
- 6.2.11 本校存放個人資料檔案之應用系統，於開發時，應避免以真實個人資料進行測試。如需使用，應於完成測試作業後立即移除，或將可辨識的個人資料修改為無法辨識之模糊資訊。
- 6.2.12 本校因協議或契約而分享個人資料檔案時，應於書面協議或契約書

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

中說明雙方使用資料的目的及其相關限制，且不逾越「個資法」之規範，並依據「國立宜蘭大學個人資料文件管理程序書」

(NIU-PIMS-B-002) 填寫「國立宜蘭大學個人資料使用資訊服務申請表」(NIU-PIMS-D-005) 提出申請，須經權責單位主管核准方可提供。

6.2.13 本校應每年定期由個人資料檔案權責人員維護資料之正確性，或依當事人之請求更新或補充其個人資料，並應於個人資料變更後，通知曾提供利用之第三方。當新增涉及處理個人資料的流程或系統，應經過審查避免記錄任何錯誤或過時的個人資料。

6.2.14 個人資料正確性如有爭議者，應主動停止處理或利用，但因執行職務或業務所必須或經當事人書面同意，並經註明其爭議者，不在此限。

6.2.15 本校之個人資料檔案應依據「個資法」，對個人資料之定義區分一般及特種資料，並評估其影響程度。

6.2.16 本校應主動或依當事人之請求補充、更正、停止蒐集、停止處理、停止利用或刪除個人資料。受理當事人之請求應於 30 日內為准駁之決定，必要時得予延長，延長期間不得逾 30 日，並應將原因以書面通知請求人。

6.3 個人資料之利用控管原則

6.3.1 個人資料的利用應先確認利用的目的是否和原先蒐集的特定目的相

個人資料蒐集、處理、利用與安全管理程序書				
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次
				1.2

同。

6.3.2 含有個人資料之電子資料或紙本文件，主辦工作職掌外之讀取、列印、存檔、交換及分享等處理及利用行為，應依據「國立宜蘭大學個人資料文件管理程序書」(NIU-PIMS-B-002)填寫「國立宜蘭大學個人資料使用資訊服務申請表」(NIU-PIMS-D-005)經核准後方可執行，以建立授權、監督及行為記錄機制。

6.3.3 公務文書及紙本郵件應有專人負責收發。

6.3.4 使用影印機、印表機、傳真機、掃描機或多功能事務機處理個人資料後，應立即將資料取走。

6.3.5 含有個人資料之報廢紙張不得回收及再利用。

6.3.6 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，放置於上鎖之抽屜或儲櫃內，以避免個人資料外洩。

6.4 個人資料之傳輸控管原則

6.4.1 個人資料採電子檔案進行傳輸時，應視檔案之機密等級適時採取資訊加密技術傳輸執行（如壓縮軟體加密），且解密金鑰須分開傳送。

6.4.2 個人資料以紙本方式進行傳輸時，應視文件之機密等級適時採取彌封或專人遞送等其它具保密機制之傳遞方式進行。

6.4.3 個人資料以傳真模式進行傳輸時，應於傳真前通知對方，並於傳真後立即與對方進行確認。

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

6.4.4 個人資料傳輸至境外時，應簽訂書面協議或契約，以明訂管理責任，並確保傳輸行為、協議或契約符合相關法律及教育部之規範。

6.5 個人資料之儲存控管原則

6.5.1 本校處理、儲存個人資料檔案之資訊設備，應由專人負責保管與維護。

6.5.2 各單位儲存個人資料檔案之磁碟、磁帶及紙本等相關儲存媒體，需指定專人管理，並置於實體保護之環境，例如上鎖之儲櫃、防潮箱或銀行保險箱等。

6.5.3 由廠商協助維修儲存個人資料檔案之電腦設備時，應指派專人在場確保資料的安全。

6.5.4 儲存個人資料檔案之儲存媒體，應建立定期備份或備援機制。

6.5.5 本校個人資料檔案之保存期限，應依據「國立宜蘭大學個人資料風險評鑑與管理程序書」(NIU-PIMS-B-003) 各單位「國立宜蘭大學個人資料檔案清冊」(NIU-PIMS-D-007) 中「保存期限」欄位辦理。

6.6 個人資料之銷毀控管原則

6.6.1 個人資料檔案超過保存期限，除審核有無永久保留外，應依規辦理銷毀作業。

6.6.2 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，應刪除其所儲存之個人資料檔案。

6.6.3 超過保存期限之個人資料檔案應填寫「國立宜蘭大學個人資料紀錄

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

銷毀申請單」(NIU-PIMS-D-006)，經權責單位主管核准後辦理銷毀。

6.6.4 另超過保存期限之個人資料檔案，當基於正當理由該單位主任核准後，暫不銷毀時，應填寫於「國立宜蘭大學超過保存期限之個人資料檔案清冊」(NIU-PIMS-D-011)，並訂定預定銷毀期限，以進行控管。

6.6.5 個人資料檔案銷毀時，應依下列方式處理：

6.6.5.1 紙本若屬大量銷毀應指定專業廠商並有相關安全控管措施
(如：人員全程陪同或全程錄影監控)。

6.6.5.2 紙本若少量則應以碎紙機銷毀。

6.6.5.3 若為電子檔案，應依規範辦理刪除，並清除「資源回收筒」。

6.6.6 本程序書施行前已存在之個人資料檔案保存期限應至少保留至檔案原定之保存年限後，依規定辦理銷毀作業。

6.6.7 儲存媒體如要報廢或移作他用時，媒體上之個人資料必須清除，並應採用以下任一種合宜之措施進行銷毀：

(1) 硬碟或隨身碟

利用資料清除軟體或以實體破壞方式，清除資料內容。

(2) 光碟或磁帶

應進行實體之破壞，使其無法使用。

6.6.8 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之

個人資料蒐集、處理、利用與安全管理程序書				
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次
				1.2

請求，刪除、停止處理或利用該個人資料，但因執行職務或業務所必須或經當事人書面同意者，不在此限。

- 6.6.9 個人資料蒐集之特定目的消失或期限屆滿時，由權責單位確定已無保存之必要後，應填寫「國立宜蘭大學個人資料紀錄銷毀申請單」（NIU-PIMS-D-006）經權責單位主管核准後辦理刪除或銷毀。

6.7 個人資料之委外控管原則

- 6.7.1 委外處理個人資料檔案，應於委外合約及「國立宜蘭大學委外專案個人資料保護條款」（NIU-PIMS-D-024）載明所處理之個人資料保密義務、個人資料安全相關責任及違反之罰則。
- 6.7.2 受本校委託處理個人資料之委外廠商，在簽訂正式書面協議或契約及簽訂「委外廠商保密切結書」（NIU-ISMS-D-024）後，本校保留個人資料保護管理相關作業之稽核權，以確保當事人之個人資料安全。
- 6.7.3 若委外廠商將個人資料處理作業進行再轉包，所簽訂之書面協議或契約應有與該委外廠商相同之安全控管措施，委外廠商亦應保留對轉包廠商進行相關安控措施之稽核權。
- 6.7.4 與第三方廠商所簽訂正式書面協議或契約中，應明確陳述契約終止時，相關個人資料應被銷毀，或交還本校或業務承辦單位。
- 6.7.5 機關得針對廠商的個人資料安全管理措施實施情形派員進行實地訪查或委託專業人員進行查核，廠商應予配合。機關於訪查或查核後，

個人資料蒐集、處理、利用與安全管理程序書					
文件編號	NIU-PIMS-B-004	機密等級	限閱	版次	1.2

認有缺失，得以書面敘明理由請廠商限期改善。

6.8 第三方揭露個人資料之要求

6.8.1 本校取得當事人的同意或其他法令之特別規定，始得將個人資料揭露予第三方或使用於蒐集目的以外之其他用途。

- (1) 針對要求資料揭露的第三方，驗證其所宣稱的身分、存取個人資料權利及法源依據的真實性。
- (2) 於可行時，僅揭露最少數量的個人資料予第三方。
- (3) 留存資料揭露的作業紀錄，以追蹤個人資料揭露之軌跡，並包含其合法證明。

6.8.2 若需要於本校對外網站或網頁公布個人資料時，應進行適當之遮蔽或僅公告適當之資訊，並經權責主管核准後依相關法律及規範處理。

7 相關表單

- 7.1 「國立宜蘭大學個人資料使用資訊服務申請表」(NIU-PIMS-D-005)。
- 7.2 「國立宜蘭大學個人資料提供同意書」(NIU-PIMS-D-010)。
- 7.3 「國立宜蘭大學隱私權政策聲明」(NIU-PIMS-D-014)。
- 7.4 「國立宜蘭大學個人資料檔案清冊」(NIU-PIMS-D-007)。
- 7.5 「國立宜蘭大學超過保存期限之個人資料檔案清冊」(NIU-PIMS-D-011)。
- 7.6 「委外廠商保密切結書」(NIU-ISMS-D-024)。
- 7.7 「國立宜蘭大學委外專案個人資料保護條款」(NIU-PIMS-D-024)。