國立宜蘭大學

個人資料安全控管作業說明書

機密等級：限閱

文件編號：NIU-PIMS-C-001

版　　次：1.1

發行日期：110 年 12 月 01 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
1.1	110 年 12 月 01 日	3、4	游育豪	1. 頁 3、4 將「國立宜蘭大學員工個人資料保密同意書」（NIU-PIMS-D-021）變更為「保密切結書」（NIU-ISMS-D-016） 2. 頁 4 將「國立宜蘭大學委外廠商保密切結書」（NIU-PIMS-D-022）變更為「委外廠商保密切結書」（NIU-ISMS-D-024）

目錄

個人資料安全控管作業說明書					
文件編號	NIU-PIMS-C-001	機密等級	限閱	版次	1.1

1 目的

依據「個人資料保護法」、「個人資料保護法施行細則」及國立宜蘭大學（以下簡稱本校）「國立宜蘭大學個人資料保護管理政策」（NIU-PIMS-A-001）等相關規定，制訂本校個人資料安全控管程序，以確保個人資料受適當的控管與監視，防止不當管控而造成資料外洩之風險。

2 參考依據

2.1 「國立宜蘭大學資訊資產管理程序書」（NIU-ISMS-B-003）。

2.2 「國立宜蘭大學實體安全管理程序書」（NIU-ISMS-B-006）。

2.3 「國立宜蘭大學通信與作業管理程序書」（NIU-ISMS-B007）。

2.4 「國立宜蘭大學存取控制管理程序書」（NIU-ISMS-B008）。

2.5 「國立宜蘭大學安全事件管理程序書」（NIU-ISMS-B-011）。

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

2.7 「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）。

2.8 「國立宜蘭大學個人資料保護緊急應變處理作業說明書」（NIU-PIMS-C-002）。

3 適用範圍

本校個人資料（含書面、電子個人資料）均適用之。

4 權責

本校全體同仁（含正式員工、約聘僱人員、工讀生與委外廠商人員）均應遵守本程序書之相關規定，以確保本校相關個人資料（含書面、電子個人資料）之安全。

5 作業說明

5.1 實體與環境的安全：電腦機房門禁管制、電腦機房安全管理及個人電腦安全管理，依「國立宜蘭大學實體安全管理程序書」(NIU-ISMS-B-006)、「國立宜蘭大學資訊資產管理程序書」(NIU-ISMS-B-003）辦理。

5.2 存取管制：個人資料相關之檔案、系統、資料庫、網路、設備存取權限管理，及帳號、密碼安全設定原則與管理，依「國立宜蘭大學存取控制管理程序書」(NIU-ISMS-B008）辦理。

5.3 個資/資安事件通報：發生個資事故亦屬資安事件除依「國立宜蘭大學個人資料保護緊急應變處理作業說明書」(NIU-PIMS-C-002）辦理外，亦須依「國立宜蘭大學安全事件管理程序書」(NIU-ISMS-B-011）辦理。

5.4 軌跡紀錄管理：個人資料使用紀錄、軌跡資料管理依「國立宜蘭大學個人資料文件管理程序書」(NIU-PIMS-B-002）辦理。

5.5 個人資料檔案、媒體、設備刪除、銷毀、移轉他用：電子式個人資料刪除、銷毀及存有個人資料之媒體、設備報廢、移轉他用依「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）辦理。

5.6 日常作業管理：可攜式電腦、儲存媒體安全管理、個人資料備份管理、

惡意軟體（程式）之防範、個人資料傳遞交換、檔案分享軟體管制、弱點掃描及漏洞修補管理、個人資料檔案加密作業，依「國立宜蘭大學通信與作業管理程序書」(NIU-ISMS-B007)，及「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）辦理。

5.7 一般安全控制

5.7.1 人員安全與教育訓練

5.7.2 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。

5.7.3 本校同仁於到職時應簽署「保密切結書」(NIU-ISMS-D-016)，並恪盡保密之責。

5.7.4 每年應對組織內部人員規畫訓練課程，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。

5.7.5 為確保教育訓練執行之成效，可採行隨堂抽問、案例討論、習題演練或隨堂測驗等方式進行成效評估。

5.7.6 本校個人資料保護安全教育訓練一般人員至少 3 小時，其簽到表及執行成效等紀錄應由個資保護執行小組留存備查。

5.8 委外管理

5.8.1 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」及本校相關規定，且不得對外透露。廠商及專案人

員並應簽署「委外廠商保密切結書」(NIU-ISMS-D-024)。

5.8.2 委外廠商履行契約所使用之軟體不得違反著作權法之規定，若因使用非法軟體造成本校單位個人資料外洩，委外廠商須承擔所有法律責任。

5.8.3 委外廠商於專案服務期間所使用之工具軟體及作業執行紀錄，本校有權進行稽核，廠商不得異議。

5.8.4 於專案期間，本校應透過稽核等方式監督委外廠商之個人資料管理作法，如個人資料蒐集、處理、利用、傳輸與銷毀之管理情形。

5.8.5 委外廠商如因其員工業務過失，造成本校損害時，委外廠商需負賠償或復原責任。

5.8.6 委外廠商進行系統開發、測試與維護時，未經權責主管許可，不得複製或攜出本校保有之教、職、員、工、生等相關個人資料。

5.8.7 提供委外廠商測試之資料，應將個人資料欄位內容轉換為虛擬資料或移除。

6 相關表單

6.1 「委外廠商保密切結書」(NIU-ISMS-D-024)。

6.2 「保密切結書」(NIU-ISMS-D-016)。