國立宜蘭大學

個人資料稽核作業程序書

機密等級：限閱

文件編號：NIU-PIMS-B-006

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

個人資料稽核作業程序書					
文件編號	NIU-PIMS-B-006	機密等級	限閱	版次	1.0

1 目的

藉由個人資料保護安全稽核作業，瞭解國立宜蘭大學（以下簡稱本校）執行個人資料保護安全控制程序符合「個人資料保護法」及「國立宜蘭大學個人資料保護管理政策」（NIU-PIMS-A-001）之規定與要求，供本校持續維護個人資料保護管理制度之參考，特訂定本程序書。

2 參考依據

2.1 個人資料保護法。

2.2 個人資料保護法施行細則。

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

2.4 「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

個人資料管理制度之定期、不定期稽核作業。

4 權責

4.1 個人資料保護推動委員會（以下簡稱個保會）

審核「國立宜蘭大學個人資料管理制度內部稽核計畫」（NIU-PIMS-D-016）及「國立宜蘭大學個人資料管理制度內部稽核報告」（NIU-PIMS-D-018）。

4.2 個資保護稽核小組

負責擬訂「國立宜蘭大學個人資料管理制度內部稽核計畫」（NIU-PIMS-D-016）、辦理內部稽核作業並產出「國立宜蘭大學個人資料管理制度內部稽核報告」（NIU-PIMS-D-018）。

4.3 受稽單位

配合各項查核與其他稽核作業。

5 定義

5.1 外部稽核

由獨立之第三方單位，進行個人資料管理制度之查核。

5.2 內部稽核

對個人資料處理作業是否符合所建立之個人資料管理制度所進行之稽核作業。

5.3 個人資料管理制度內部稽核計畫

稽核人員依據稽核目的，並參考前次查核與外部稽核追蹤事項所製作之工作計畫。

5.4 個人資料管理制度內部稽核底稿

稽核人員依稽核計畫實施書面查核或進行實地查核，並確實記錄所發現之情況，以做為稽核之佐證並留下稽核軌跡。

5.5 個人資料管理制度內部稽核報告

包括背景描述、稽核期間、稽查項目（範圍）、稽核方法與標準、稽核結果、改進建議等內容。

6 作業說明

6.1 法規要求之符合性

6.1.1 整體個人資訊管理制度之規劃、設計、建置及實施，均須遵循政府

頒布之相關法令規章。包括：

6.1.1.1 個人資料保護法。

6.1.1.2 個人資料保護法施行細則。

6.1.2 對於個人資料之蒐集、整理、傳遞與使用之管理，應建立嚴謹之控管程序，以確實遵循「個人資料保護法」對個人資訊隱私及資料保護之規範。

6.1.3 含個人資料之重要業務（如人事資料、學籍資料及會計資料等）應建立作業紀錄及稽核軌跡項目、保存期限，留存期限應遵循相關規範辦理。

6.2 個人資料保護政策符合性的審查

各管理者應確保在其責任範圍內的所有安全程序是被正確地執行，並且應定期審查相關資訊作業，以確保符合「個人資料保護管理政策」及相關作業規範。

6.3 稽核人員之要求

為確保稽核過程的客觀性與獨立性，稽核之執行應由非受稽人員擔任。可由下列方式組成稽核團隊執行稽核活動，依權責辦理各項個人資料保護稽核事務。

6.3.1 聘請外部個人資料保護顧問。

6.3.2 審定合格之稽核人員，如具有個人資料國際認證主導稽核員訓練證書者或已接受個資內部稽核相關訓練者擔任。

6.4 個人資料管理制度內部稽核

6.4.1 個人資料管理制度內部稽核人員應定期參加個人資料保護教育訓練，以持續加強個人資料保護專業能力與查核技巧。

6.4.2 個人資料管理制度內部稽核每年至少辦理 1 次，並可視需要不定期舉行，當個人資料管理制度發生重大變更後，應立即執行稽核作業。

6.4.3 個資保護稽核小組應事先擬定稽核計畫，闡明稽核範圍與項目，陳核執行秘書核可後，方得實施。

6.4.4 內部稽核報告由個資保護稽核小組彙整後，呈報執行秘書核定。內部稽核報告所列建議改善事項，應辦理追蹤複檢。

6.4.5 稽核紀錄與報告（如稽核工作底稿與內部稽核報告），應由個資保護稽核小組妥善保管，必要時得提供外部稽核時之參考。

6.4.6 受稽部門應尊重及支持個資保護稽核小組成員，誠實答覆稽核人員所提問題，並接受調閱有關紀錄、報告及文件。

6.4.7 稽核人員應依照查核發現之情況於稽核工作底稿中標示符合度，並概略描述查核項目之現況說明及結果。

6.4.8 符合度判定標準如下：

6.4.8.1 不適用：凡該查核項目不包含於現行個人資訊管理制度範圍內者。

6.4.8.2 不符合：查核過程中該項目發現任何缺失，或稽核人員提出需改進事項者，該項目即評為不符合。

6.4.8.3　符合：該查核項目未發現任何缺失者，該項目即評為符合。

6.4.9 內部稽核報告之缺失與建議事項，應訂定改善方案據以執行，並由個資保護稽核小組辦理複核工作。

6.4.10 遇有重大個人資料安全事故，如個人資料外洩、系統遭受入侵、人員違法事件或其他足以影響本校聲譽之情事等，個資保護稽核小組均應辦理相關之內部稽核業務，並納入矯正預防程序追蹤管理。

6.5 外部稽核

6.5.1 配合主管機關之要求，進行外部稽核作業。

6.5.2 本校應依組織需求，考量是否委託超然獨立之外部稽核單位，對日常作業個人資料保護相關規定來進行稽核。

6.6 矯正預防處理

受稽部門於接獲內部稽核報告後，應依據「亞立宜蘭大學個人資料矯正預防管理程序書」（NIU-PIMS-B-007）之規定實施矯正，並於十五個工作天內將該單位之缺失原因分析及擬採行之矯正與預防措施填列於「國立宜蘭大學個人資料管理制度矯正預防處理單」（NIU-PIMS-D-019）內，經單位權責主管核定後回覆個資保護稽核小組。

7 相關表單

7.1 「國立宜蘭大學個人資料管理制度內部稽核計畫」(NIU-PIMS-D-016)。

7.2 「國立宜蘭大學個人資料管理制度內部稽核底稿」(NIU-PIMS-D-017)。

7.3 「國立宜蘭大學個人資料管理制度內部稽核報告」(NIU-PIMS-D-018)。