國立宜蘭大學

個人資料保護緊急應變處理作業說明書

機密等級：限閱

文件編號：NIU-PIMS-C-002

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

個人資料保護緊急應變處理作業說明書					
文件編號	NIU-PIMS-C-002	機密等級	限閱	版次	1.0

1 目的

國立宜蘭大學（以下簡稱本校）為建立個人資料事故管理作業準則，並規範事故處理之作業事項，針對個人資料侵害之情形，決定其影響範圍及緊急程度，並能快速解決問題，確保事故能有效處理，特訂定本說明書。

2 參考依據

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

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

2.3 「國立宜蘭大學個資保護內控程序」。

3 適用範圍

無論來自於人為故意或不經意的，或不可抗力的因素，任何導致本校個人資料管理異常狀況均適用之。

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 負責個資事故處理與預防。

4.1.2 負責個人資料保護資源協調與流程改善。

4.1.3 負責監督重大／緊急事故及稽核缺失的矯正措施之實施，並確認預防措施之有效性。

4.2 個保會執行秘書

4.2.1 個人資料保護業務之協調聯繫及緊急應變通報。

4.2.2 督導個資事故通報應變作業執行狀況。

4.3 個資保護執行小組

4.3.1 「個人資料保護法」(以下簡稱個資法）第十條及第十一條第一項至第四項所定依法或依當事人請求事項之考核。

4.3.2 「個資法」第十一條第五項及第十二條所定通知事項之考核。

4.3.3 本校個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。

4.3.4 辦理事件辨識、抑制、排除及回復作業。

4.3.5 辦理本校各單位之個人資料損害預防及危機處理應變之通報。

4.3.6 協助辦理本校各單位之個人資料保留與處置。

4.3.7 建立並統籌個資保護聯絡窗口。

4.3.8 由個保會指派圖書資訊館擔任本校個人資料管理窗口。

4.4 本校所有同仁

4.4.1 協助配合各類個資事故之報告與處理。

4.4.2 應瞭解個資事故應變通報流程，並協助通報相關權責單位。

4.5 委外廠商與人員

4.6 遵守法規及本校相關個人資料保護管理制度規範。

5 定義

個資事故,係指單一或一連串機率可能危害與威脅個資安全之非蓄意或非預期的個資事故；簡而言之，泛指對本校已構成傷害之事故。例如：

5.1 個人資料檔案遭遇竊取、竄改、毀損、滅失或洩漏等相關事故。

5.2 洩漏個人資料或違反個資政策之故意行為或重大人為疏失。

5.3 販賣個人資料圖利。

5.4 個人資料檔案遭受誤用。

5.5 超過蒐集之特定目的處理或利用。

5.6 未經同意蒐集個人資料。

5.7 個人資料未應當事人請求修改、刪除、停止使用、製給複製本及閱覽權。

6 作業說明

6.1 建立個資事故通報及受理程序

6.1.1 本校應建立完整之內部個人資料事故通報流程，當發生個資外洩時必須告知當事人並留下通報紀錄，若有通報而無相關通報記錄，事後將究責。

6.1.2 個資事故其通報方式依據本作業說明書「國立宜蘭大學個資事故通報及受理流程」(NIU-PIMS-D-023)辦理。

6.1.3 接獲個資事故通報後，需依所通報之內容進行處理，並填寫本校「國立宜蘭大學個資安全事件申訴與通報紀錄表」(NIU-PIMS-D-012)。

6.1.4 當違反個資法規定，導致個人資料被竊取、洩漏、竄改或其他侵害者，應於查明後以適當方式通知當事人。

6.1.5 應建立通報機制，確保所使用的方式（例如電話、簡訊、郵寄、E-mail 等）可以通知到當事人，並留下紀錄。

6.1.6 個資事故通報單位依據各種管道向本校個資保護聯絡窗口進行通知，由個資保護聯絡窗口應立即協同個保會召集人蒐集相關跡證，初步判斷是否為個資事件，若確定為個資事件後，將問題轉予權責單位進行處理，待權責單位處理完成後，將處理結果回覆個資保護聯絡窗口，且保留相關紀錄。

6.1.7 個資事故之當事人通報及受理程序詳「國立宜蘭大學個資事故通報及受理流程」(NIU-PIMS-D-023)。

6.1.8 若確實是由內部處理不當導致當事人個人資料洩漏、損失及毀損等情形，將依「個資法」第四章第二十八條進行損害賠償。

6.2 個資事故通報

6.2.1 各單位於發現個資遭侵害時，應通知個資保護聯絡窗口應立即協同個保會召集人蒐集相關跡證，初步判斷是否發生個資事故判斷是否發生個資事故。

6.2.2 若個資事故成立，根據判斷結果，依個資事故分級與應變作業表的通報流程處理。

6.2.3 個資事故分級與應變作業表

事故等級	符合下列任一條件	應變單位與處理
一級事故	1、遭受未經授權刪除、修改、外洩之個資筆數 50 筆以下。 2、事故涉及一般個資，但已採加密、遮蔽、設定無法讀	立即通報聯絡窗口，並協同事故發生單位共同處理。

	取或其他方式加以控管。	
二級事故	1、遭受未經授權刪除、修改、外洩之個資筆數達 51 筆以上，未達 1000 筆。 2、事件涉及一般個人資料，且未以加密、遮蔽、設定無法讀取或其他方式加以控管。 3、外洩之個人資料涉及特種個人資料或財務細節，但已採加密、遮蔽、設定無法讀取或其他方式加以控管。 4、事件已受到媒體關注(媒體詢問，尚未報導)。	立即通報聯絡窗口及個保會召集人，如有涉及資訊安全事故，亦需通報本校資訊安全官，成立個資事故應變小組，成員須包含：個保會召集人、執行秘書、秘書室、人事室、事件發生單位的個資保護小組執行人員及其他相關單位人員。
三級事故	1、遭受未經授權刪除、修改、外洩之個資筆數超過 1000 筆。 2、外洩之個資涉及特種個資或財務細節，且資料未以加密、遮蔽、設定無法讀取或其他方式加以控管。 3、事件已受到媒體報導。 4、事件已接獲司法機關通知。	立即通報聯絡窗口及個保會召集人，如有涉及資訊安全事故，亦需通報本校資訊安全官，成立個資事故應變小組，成員須包含：個保會召集人、執行秘書、秘書室、人事室、事件發生單位的個資保護小組執行人員、其他相關單位人員及本校法律顧問。

6.2.4 若聯絡窗口與個保會召集人判定事故不成立，即告知通報人及事件發生單位，並送個保會個保會定期會議討論。

6.2.5 若聯絡窗口與個保會召集人判定事故成立，則需依個資事故分級與應變作業表判定級別，並依分級進行相關流程。

6.2.6 個資事故處理完成，需由個保會複核並判斷個資事故處理方式作業是否得當，若處理不得當，則退回緊急處理小組再進行事故處

理。

6.2.7 若個保會判定處理得當，由聯絡窗口完成個資安全事件申訴與通報紀錄表，並依資訊安全事件與應變作業程序通報，並告知通報人以及當事人（必要時，並需通報主管機關）。

6.3 通報原則

6.3.1 個資事故發生時，應依通報順序逐級陳報。

6.3.2 當上述任何一層級人員無法依層級順序被通報時，負責通報人員應往上一層級逕行陳報，以確保通報程序之即時性。

6.4 判斷個資事故

6.4.1 個資保護聯絡窗口接獲相關個資案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。

6.4.2 若經判斷為個資事故，事故處理之業管單位應立即依據「個資事故分級與應變作業表」，啟動個資應變措施相關處理作業。

6.4.3 個人資料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，確實記錄於「國立宜蘭大學個資安全事件申訴與通報紀錄表」(NIU-PIMS-D-012)，並陳報權責單位主管審核。

6.5 記錄個資事故，啟動應變措施

個資應變措施應符合限制、處理、復原等三階段的事故處理原則，說明如下：

6.5.1 針對可即時解決之個資事件，業務權責單位陳報主管審核後，並通報個資保護聯絡窗口。

6.5.2 若個資遭到人為竄改或失竊等涉及民、刑事案件時，應即時通報警政或檢調單位請求處理。

6.5.3 事故處理作業所留存之相關紀錄應至少保留結案後 5 年備查。

6.6 確認狀況排除

6.6.1 個資事故處理人員於處理完成後，應確認應變措施之有效性，並回報個資管理窗口及業務權責單位主管，視情況調整應變措施。

6.6.2 個資事故發生之業務權責單位主管於初步認定事故排除後，仍應嚴密監控相關資訊，並進行必要之安全清查，防止潛伏之可疑行為再發生。

6.6.3 個資事故確認排除後，業務權責單位應再回報個資保護聯絡窗口後續處理情形，且由其通知本校受事故影響之相關單位或回報上級單位。

6.6.4 個資保護聯絡窗口應留存紀錄，並決定是否通報主管機關或要求業務權責單位通知當事人。

6.6.5 業務權責單位應儘速將損失彙整後通知個資保護聯絡窗口，由個資保護聯絡窗口，視需求協助本校召集人對外說明情況與處置方式。

6.7 檢討及改善

6.7.1 個資事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。

6.7.2 事故發生單位應於事故處理完畢後，進行相關矯正預防措施，填寫「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)，避免同類型之個資事故重複發生。

6.7.3 各單位權責主管應監督個資事故之後續處理及安全控制之有效性。

6.7.4 個資事故之發生單位應為個人資料稽核作業之重點，並列入追蹤管理。

6.7.5 由個人資料聯絡窗口彙整「國立宜蘭大學個資安全事件申訴與通報紀錄表」(NIU-PIMS-D-012)，並在無牽涉個人隱私與本校業務機密之情況，將事件發生原因、過程、處理方式、注意事項及改善建議等內容，以網站或電子郵件等方式提供予本校員工，以做為內部個人資料保護安全宣導及事故預防之參考。

7 相關表單

7.1 「國立宜蘭大學個資事故通報及受理流程」(NIU-PIMS-D-023)。

7.2 「國立宜蘭大學個資安全事件申訴與通報紀錄表」(NIU-PIMS-D-012)。

7.3 「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)。