資通安全事件管理程序書

文件編號：NDHU-I-B-12
機密等級：限閱

單　　位：國立東華大學
版　　次：1.3
發行日期：114 年 10 月 2 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	112.11.20	ALL	劉維忠	初版發行。
1.1	113.12.26	P.5-9	蕭澤宇	5.4、5.5 名稱修正。
1.2	114.4.22	P.2、P.4	蕭澤宇	5.2.1、5.4 名稱修正。
1.3	114.10.2	P.8	蕭澤宇	B,C 級保存範圍修正、新增資安事件數位證據保全標準作業程序

目錄

1 目的

為建立國立東華大學（以下簡稱「本校」）資通安全事件處理程序，降低因事件所造成之損害，從而建立事件學習機制，藉以避免類似資通安全事件重複發生。

2 適用範圍

本校承辦相關資通業務之資通安全事件管理，以及威脅情資之獲取與分享等，皆屬本程序書之範疇。

3 權責

3.1 「資通安全處理小組」: 審核本校「NDHU-I-B-12-01 資通安全事件通報與應變作業流程圖」，及督導資通安全事件之處置。

3.2 「資通分組」: 研擬資通安全事件通報流程及緊急應變處理程序。

3.3 發現人員：本校所有同仁，包括正式員工、約聘僱人員、自然人、借調人員、工讀生、委外服務廠商（人員）、協力廠商（人員）、訪客及與本校連線作業之機關全體同仁、資料使用者(含保管者)等均適用之。

3.4 權責單位：執行資通安全事件之分析及處理。

3.5 單位權責主管：督導資通安全事件通報、處理及分析作業。

3.6 緊急應變處理分組：於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。

3.6.1 確定事件影響範圍，並評估損失。

3.6.2 協助資通安全事件之通報、處理及分析作業。

4 名詞定義

4.1 資通安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

4.2 天然災害：颱風、水災、地震等。

4.3 突發事件：火災、爆炸、重大建築災害及資通網路骨幹（主幹寬頻）中斷事件等。

5 作業說明

5.1 資通安全事件之管理

5.1.1 應建立資通安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速、有效處理資通安全事件。

5.1.2 資通安全事件之處理程序，應視需要納入下列事項：

5.1.2.1 電腦稽核相關證據之蒐集。

5.1.2.2 導致資通安全事件原因之分析。

5.1.2.3 防止類似事件再發生之補救措施。

5.1.2.4 與受影響之使用者進行溝通及說明。

5.1.3 電腦稽核相關證據應以適當方法保護，以利下列管理作業：

5.1.3.1 作為研析問題之依據。

5.1.3.2 作為研析是否違反契約或資通安全規定之證據。

5.1.3.3 作為與委外廠商協商如何補償之參考。

5.1.4 應依據「NDHU-I-B-12-01 資通安全事件通報與應變作業流程圖」處理資通安全事件。相關作業程序應考量下列事項：

5.1.4.1 考量單位資源，於最短的時間內，確認復原後之系統及相關安全控制是否完整及正確。

5.1.4.2 向管理階層報告處理情形，並檢討、分析資通安全事件。

5.1.4.3 緊急處理步驟應詳實記載，以備日後查考。

5.2 通報應變組織

5.2.1 本校參據行政院頒修「各機關資通安全事件通報及應變處理作業程序」，成立「緊急應變處理分組」，以本校「資通安全暨個人資料保護處理小組」相關編組人員擔任，於平時進行演練，並於發生資通安全事件時，依事件級進行通報及應變作業，相關編組對應如下：

事件區分 人員	第一級、第二級 資通安全事件	第三級、第四級 資通安全事件
事件指揮官	「資通分組」組長	本校資通安全處理小組召集人(資通安全長)或其授權人員
新聞官/組	機關/單位對外發言人員或單位主管	
執行秘書	「資通分組」成員或資安專職人員	「資通分組」組長
情資及計畫組組長	「資通分組」成員或資安專職人員	「資通分組」組長
應變執行組組長	「資通分組」成員或資安專職人員	「資通分組」組長
後勤調度組組長	「資通分組」成員或資安專職人員	「資通分組」組長
財務行政組組長	本校主計室或秘書室主管	

5.2.2 人員職掌

5.2.2.1 事件指揮官：

綜理全般業務，直接督導各單位聯絡人員及機關新聞官/組。

5.2.2.2 新聞官/組

為資通安全事件對外發布新聞或說明之單一窗口，負責綜整與定期更新訊息及擬溝通計畫，視事件需要由事件指揮官或其授權人員擔任新聞官或分組代表。

5.2.2.3 執行秘書

為事件指揮官幕僚，負責督辦通報應變分組各項業務。

5.2.2.4 情資及計畫組

負責辦理下列事宜：

5.2.2.4.1 資通安全事件通報及情資分享：透過監控資通安全事件通報及情資分享中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件階段通報，分享惡意程式 IoC 及相關威脅情資等。

5.2.2.4.2 應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。

5.2.2.4.3 本分組由機關資通安全專責人員、資訊人員及委外廠商或外部專家組成，上級或相關機關，亦應視情況或納入政風單位派員參與，以提供必要之支援協助。

5.2.2.5 應變執行組

負責辦理下列事宜：

5.2.2.5.1執行損害控制：依據情資及計畫組研擬之應變策略，調度資通安全人員執行災害搶救及損害管制，防止次波攻擊及擴散。

5.2.2.5.2復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。

5.2.2.5.3跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

5.2.2.6 後勤調度組

負責辦理下列事宜：

5.2.2.6.1事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡意

中繼站。

5.2.2.6.2提出改善建議：依據事件調查根因，提出短、中、長期改善建議。

5.2.2.6.3彙整改善報告。

5.2.2.6.4撰寫調查、處理及改善報告。

5.2.2.6.5追蹤管考：針對機關單位已結案或未結案事項，如有未盡改善事宜，將另案追蹤管考。

5.2.2.7 財務行政組

視事件需要由本校主計室或秘書室組成，負責辦理預算調撥及提供行政支援事宜。

5.3 威脅情資

5.3.1 本校應蒐集、分析與資通安全威脅有關的威脅情資，運用上級或其他機關通報機制，以「NDHU-I-B-12-03_威脅情資彙處表」進行管控及處理。

5.3.2 所蒐集或分析有關現有或新出現威脅的資訊，將發布或通知本校各單位並分享各管理處及回報知悉及採取行動，以防止威脅對組織造成傷害。

5.4 通報程序

5.4.1 疑似資通安全事件發生時，發現人員應通報資訊權責單位，並副知單位權責主管與「資通分組」，相關通報流程應依據附件之「資通安全事件通報程序」辦理。

5.4.2 資訊權責單位於收到通知後，研判是否為資通安全事件。若：

5.4.2.1 判定為非資通安全事件時，則將結果回覆予發現人員，並將處理結果紀錄於「NDHU-I-B-06-02 異常狀況處理紀錄表」。

5.4.2.2 判定為資通安全事件時，初估事件處理時間，並副知單位權責主管與「資安業務執行小組」。

5.4.2.3 資通安全事件依影響等級區分為 4 個級別，由輕至重分別為「1 級」、「2 級」、「3 級」及「4 級」。

5.4.2.3.1 1 級事件，符合下列任一情形者：

5.3.2.3.1.1 非核心業務一般資料遭洩漏。

5.3.2.3.1.2 非核心業務系統或資料遭輕微竄改。

5.3.2.3.1.3 非核心業務運作遭影響或短暫停頓，於可容忍中斷時間 內回復正常運作。

5.4.2.3.2　2 級事件，符合下列任一情形者：

5.3.2.3.2.1 非屬密級或敏感之核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。

5.3.2.3.2.2 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統 或資料遭輕微竄改。

5.3.2.3.2.3 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

5.4.2.3.3　3 級事件，符合下列任一情形者：

5.3.2.3.3.1 密級或敏感資料遭洩漏。

5.3.2.3.3.2 核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改。

5.3.2.3.3.3 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

5.4.2.3.4　4 級事件，符合下列任一情形者：

5.3.2.3.4.1 國家機密資料遭洩漏。

5.3.2.3.4.2 關鍵資訊基礎設施系統或資料遭嚴重竄改。

5.3.2.3.4.3 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

5.4.3 資訊權責單位確認資通安全事件後，應於 1 小時內，至教育機構資安通報平台通報登錄資安事件細節、影響等級及支援申請等資訊並留存相關紀錄。另，評估該事件是否影響其他政府機關(構)運作，需橫向通報相關單位。

5.4.4 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後 1 小時內，與教育部和台灣學術網路危機處理中心(TACERT)聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至教育機構資安通報平台補登錄通報。

5.4.5 進行資安事件處理，「3」、「4」級事件須於 36 小時內完成復原或損害管制；「1」、「2」級事件須於 72 小時內完成復原或損害管制。

5.4.6 完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理辦法及完成時間。

5.4.7 決策處理：

5.4.7.1 當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時，由事件發生單位自行處理，並將處理後狀況通知單位權責主管與資訊權責單位。

5.4.7.2 事件處理過程中如發現所造成之影響大於原先判定時，事件發生單位應立即通報資訊權責單位，並重新執行事件分析及辨識。

5.4.7.3 應參考「資通安全事件通報及應變辦法」之資通安全通報與應變作業流程，並依據資訊權責單位所提報之事件影響評估，向本校「資通安全暨個資保護執行小組」召集人建請是否向上級主管單位通報。

5.4.8 第 3 級或第 4 級資通安全事件，各機關除依前目規定通報外，應另以電話或其他適當方式通知上級機關。

5.4.9 「資通分組」之資通安全專職人員應利用「教育機構資安通報平台」，執行資通安全事件通報、應變及事件調查等任務。

5.4.10 事件根因分析時，為保存相關跡證，惡意程式得請防毒軟體或資安服務公司檢測，並上傳至 Virus Check 網站(https://viruscheck.tw/)分析，以更新或強化相關偵測及聯防機制，不宜上傳至其他平臺。

5.4.11 「資通分組」應參考「各機關資通安全事件通報及應變處理作業程序」相關流程，進行「通報資通安全事件」、「成立緊急應變處理分組與召開應變會議」、「損害控制或復原作業」、「根因分析及改善追蹤」及「跡證保存」等作業，經初判符合事件影響範圍及事件等級，應評估可能造成之損失，及預定採取之應變及復原措施，由上級機關進行審查。

5.4.12 為確保資通安全事件發生時，本校所有跡證足以進行根因分析，並視事件情形辦理其他必要之跡證保存事項。日常維運資通系統時，應依自身安全責任等級保存日誌 (log)，並考量定期備份於外部設備，其保存範圍及項目如下表：

資通安全責任等級	保存範圍	保存項目
B 級	應保存全部資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	1.作業系統日誌 (OS event log) 2.網站日誌 (web log) 3.應用程式日誌(AP log) 4.登入日誌 (logon log)
C 級	應保存全部資通系統最近六個月之日誌紀錄。	

5.4.13 有關是否啟動業務永續運作計畫，依「NDHU-I-B-13 業務永續運作管理程序書」辦理。

5.5 危機處理程序

本校應建立資安事件之事前安全防護、事中緊急應變及事後復原作業之具體機制(含 BOT 之關鍵資訊基礎設施)，至少須包括下列各項：

5.5.1 事前安全防護

5.5.1.1 應依資通系統分級作業相關規定，判定資通系統安全防護等級，並據以落實資安防護基準。

5.5.1.2 應規劃建置資通安全整體防護環境，做好本校及 BOT 廠商內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。

5.5.1.3 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。

5.5.1.4 應依資通安全防護需要，執行入侵偵測、安全檢測及弱點掃描等安全檢測工作，並訂定系統與資料備份管理辦法，以做好事前防禦準備。

5.5.1.5 應實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。

5.5.1.6 應保留資安紀錄與備份，如資通系統屬委外(含 BOT)建置管理者，應於合約內要求承商保留相關資安紀錄。

5.5.1.7 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。

5.5.1.8 無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予北區教育學術資訊安全監控中心（N-ASOC）、南區教育學術資訊安全監控中心（S-ASOC）、縣市網資訊安全維運中心（MINI-SOC）。

5.5.1.9 應建置並保存相關設備之系統日誌。

5.5.1.10 應每年定期規劃辦理資安認知教育訓練。

5.5.2 事中緊急應變

5.5.2.1 應就資安事件發生原因、影響等級、可能影響範圍、可能損失及是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。

5.5.2.2 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。

5.5.2.3 查詢通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，以尋求解決方案；如無法解決，應迅速向主管機關反應，請求提供相關技術支援。

5.5.2.4 評估資安事件對業務運作造成之衝擊，並進行損害管制。

5.5.2.5 視資安事件損壞程度，遵循本校及 BOT 廠商內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。

5.5.2.6 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。

5.5.2.7 本校於資安事件調查過程中，如需執行電腦系統之數位證據識別、蒐集、擷取、封緘及運送等作業，應依據《政府機關（構）資安事件數位證據保全標準作業程序》之相關規範辦理，以確保證據之完整性與可採信性。

5.5.2.8 如發生重大(「3」、「4」級)資安事件，應主動提供相關設備系統日誌予主管機關，俾提供相關協助。

5.5.3 事後復原

5.5.3.1 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份及資料復原等相關事宜。

5.5.3.2 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。

5.5.3.3 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。

5.5.3.4 資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊,並提送主管機關及行政院國家資通安全會報資通安全防護組檢討，以強化資通安全防護機制。

5.6 檢討及改善

5.6.1 資通安全事件確認處理完成後，資訊權責單位與事件發生單位應檢討現行管控措施之完整性，並適當修訂相關作業規範或建置及調整控制措施，必要時應召開檢討會議。

5.6.2 事件發生單位應依「NDHU-I-B-15 矯正及預防管理程序書」規定處理採取必要之

矯正及預防措施，以避免類似安全事件重複發生。

6 相關文件

6.1 資通安全事件通報及應變辦法。

6.2 各機關資通安全事件通報及應變處理作業程序。

6.3 NDHU-I-B-13 業務永續運作管理程序書。

6.4 NDHU-I-B-15 矯正及預防管理程序書。

6.5 NDHU-I-B-12-01 資通安全事件通報與應變作業流程圖。

6.6 NDHU-I-B-12-03_威脅情資彙處表。

6.7 NDHU-I-B-06-02 異常狀況處理紀錄表。

6.8

附件、資通安全事件通報程序