國立雲林科技大學資通安全事件通報及應變管理程序

目錄

壹、 目的

國立雲林科技大學(以下簡稱本校)為遵照資通安全管理法第 14 條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

三、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、 事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

（一） 聯絡電話：(07)525-0211

（二） 網路電話：98400000

（三） 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：圖書資訊處網路資安組（05-

5342601 分機:2599、2655 abuse@yuntech.edu.tw）

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、當資安事件需對外說明時，權責主管須向資訊安全長詳細報告事件情況與處置方式，並由資訊安全長對外說明，視情況向上級主管機關陳報、負責溝通協調作業，並適時提供緊急處理組必要的協助。

九、資訊安全小組成員由資訊安全委員會指派本校之資通安全相關技術人員擔任。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、 通報程序

一、疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位，並副知直屬主管。

二、權責單位於收到通知後，研判是否為資訊安全事件。若：

1. 判定為非資訊安全事件時，則將結果回覆予發現人員。
2. 判定為資訊安全事件時，初估事件處理時間，並由權責主管視情況逐層向資訊安全長報告。相關權責人員需視情況通知維護廠商及本校相關人員處理修復事宜，並持續報告處理狀況。
3. 資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。

(1) 4 級事件，符合下列任一情形者：

- 國家機密資料遭洩漏。
- 關鍵資訊基礎設施系統或資料遭嚴重竄改。
- 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。

(2) 3級事件，符合下列任一情形者：

- 密級或敏感資料遭洩漏。
- 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。
- 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。

(3) 2級事件，符合下列任一情形者：

- 核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。
- 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。
- 非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。

(4) 1級事件，符合下列任一情形者：

- 非核心業務一般資料遭洩漏。
- 非核心業務系統或資料遭輕微竄改。
- 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。

4. 權責單位於發生資訊安全事件時，應立即填具「D-041-資訊安全事件報告單」。

5. 權責單位於未達資訊安全事件且對資訊系統產生可識別之衝擊或服務偏差，應填具「D-021-異常事件紀錄表」。

6. 資訊安全事件影響等級為「3級」、「4級」為資訊安全事故，於事故處理完成後應填寫「矯正及預防處理單」並統一列管，以作為後續事故學習之文件。

三、決策處理：

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（如：電腦病毒感染），由權責單位自行處理，並將處理後狀況通知單位主管及資訊安全官。

2.處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資訊安全官報告，重新執行事件分析辨識。

3.資訊安全官應參考『教育機構資安通報應變手冊』，並依據權責單位所提報之事件影響報告，決定是否向上級主管單位通報。若需要通報，應由單位主管確認後執行。

四、有關是否啟動業務永續運作計畫，依「業務永續運作管理程序書」辦理。

陸、 應變程序

本校資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

一、 事前建置安全防護機制：

(1) 建置資訊安全管理系統及整體防護架構。

(2) 彙整及備妥資訊安全相關文件。

二、事中主動預警與緊急應變：

(1) 事件辨識：辨識事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。

(2) 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低

影響的程度及範圍。

(3) 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全委員會提出建議方案。

(4) 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

三、事後復原追蹤鑑識偵查：

(1) 後續追蹤之精神乃係檢討相關資訊安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

(2) 受損單位依復原程序實施災後復原重建。

(3) 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務中心或檢警單位申請數位鑑識（電腦、網路鑑識）。

柒、 資安事件後之評估及檢討改善機制

一、各項資訊安全事件處理完畢後，相關會辦單位須於「D-041-資訊安全事件報告單」簽名確認，並呈報權責主管。

二、權責主管需對資安事件處理結果，進行評估作業，判斷資安事件所造成之影響與衝擊已獲得改善與控制，且恢復正常運作後，於「D-041-資訊安全事件報告單」中簽名。

三、權責主管宜委派專人彙總「D-041-資訊安全事件報告單」，建立資訊安全事件學習機制，作為日後檢討與改善之依據。

四、若無法解決及處理資安事件，則持續執行各項應變計畫及危機處理作業，直至問題獲得改善與解決為止。

五、安全事件確認處理完成後，權責單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施。必要時，應召開檢討會議。

六、權責單位應依「D-046-矯正及預防管理程序書」規定處理，以避免類似安全事件重複發生。

捌、 紀錄保存

一、相關業務承辦人員應參照規範，妥善保存各項紀錄。資訊安全事件報告單應保存一年。

玖、 演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程。

(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練