國立嘉義大學資通安全事件通報應變作業計畫

計算機諮詢委員會九十六年度第二次會議（2007/12/24）提議通過
計算機諮詢委員會九十八年度第一次會議（2009/10/05）提案通過
計算機諮詢委員會九十九年度第二次會議（2010/10/20）提案通過

壹、依據及目的：

一、依據教育部「教育機構資安通報應變手冊」及本校「國立嘉義大學資訊安全管理規範實施要點」辦理。

二、為有效掌握本校資訊及網路系統疑遭破壞或不當使用時，迅速採取通報及緊急應變處置，並在最短時間內復原，以確保校務永續運作，特訂定「國立嘉義大學資通安全事件通報應變作業計畫」(以下簡稱本作業計畫)。

貳、適用範圍：

一、適用對象：

運用本校軟硬體設備及網路系統，進行電子化作業之各單位及使用者。

二、適用時機：

本校資訊及網路系統管理人員發現系統服務及功能異常，或經通知疑遭破壞或不當使用，或其他災害影響系統正常運作時，應立即依本作業計畫處理程序辦理。

參、組織及權責：

一、資訊安全長：

由行政副校長兼任，權責如下：

(一)督導本作業計畫作業執行狀況及成效。

(二)核定資安事件通報及應變處理事宜。

(三)監督通報作業、應變計畫與資安演練之實施。

二、資通安全處理小組：

(一)由本校電子計算機中心主任擔任召集人，遴選適當人員組成資通安全處理小組。

(二)小組成員包含資安聯絡人、系統管理、內部稽核等相關人員。

(三)負責執行資通安全預防措施以及資通安全事件通報、緊急應變處理等相關事項。

三、資安聯絡人：

(一)由資通安全處理小組召集人指派至少二人擔任，並於「教育機構資安通報平台」登錄聯絡資料。

(二)負責對內、對外之資通安全聯繫事宜。

(三)隨時掌握台灣學術網路危機處理中心或相關單位提供之資通安全危害通告資訊，發布資安訊息給校內各單位及系統使用者。

(四)與系統管理人員保持連繫，協同鑑定資通安全事件，並依程序進行通報作業。

四、系統管理人員：

(一)負有本校資訊及網路系統或設備管理權限之人員。

(二)負責系統維護、執行資安預防措施及重要資料備份作業。

(三)判斷系統資安徵兆，協助鑑定資通安全事件。

(四)發生資通安全事件時，採取緊急應變作業，防止事件影響擴大，保全系統記錄、稽核軌跡等事件證據。

(五)執行資通安全事件處理程序，依據授權實施系統復原作業。

五、內部稽核人員：

(一)每年實施一次資通安全內部稽核。

(二)依據資安檢核表評估整體資安風險，提出改善建議事項。

(三)協助資安事件之偵防作業。

六、系統一般使用者：

(一)泛指運用本校資訊及網路系統，進行電子化作業之各單位及使用者。

(二)負有對系統服務及功能異常反應，及配合協助資安事件通報應變作業之責任。

肆、資通安全事件分級：

資通安全事件依影響等級由重至輕分為下列級別。

一、符合下列任一情形者，屬4級事件：

(一)國家機密資料遭洩漏。

(二)國家重要資訊基礎建設系統或資料遭竄改。

(三)國家重要資訊基礎建設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。

二、符合下列任一情形者，屬3級事件：

(一)密級或敏感公務資料遭洩漏。

(二)核心業務系統或資料遭嚴重竄改。

(三)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。

三、符合下列任一情形者，屬2級事件：

(一)非屬密級或敏感之核心業務資料遭洩漏。

(二)核心業務系統或資料遭輕微竄改。

(三)核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

四、符合下列任一情形者，屬1級事件：

(一)非核心業務資料遭洩漏。

(二)非核心業務系統或資料遭竄改。

(三)非核心業務運作遭影響或短暫停頓。

五、前四項以外，下列任一情形且不影響業務運作者，屬0級事件。

(一)「教育機構資安通報平台」使用新型技術所產生之工單，經識別未確定為資安事件。

(二)其他單位所告知，經識別未確定為資安事件。

(三)教育部及區、縣網路中心檢舉信箱通告之未確定資安事件。

(四)其他違反本校校園網路使用規範或其他公約。

伍、事件通報應變處理程序

一、事件鑑定與確認：

(一)系統管理人員或使用者發現資訊及網路系統服務及功能異常反應，應立即通知資安聯絡人進行鑑定。資安聯絡人若接獲「教育機構資安通報平台」工單、其他單位告知或教育部及區、縣網路中心檢舉信箱通告之待確認事件，亦應立即通知相關系統管理人員進行鑑定。

(二)資安聯絡人協同系統管理人員分析資安徵兆或校外通知，依據事件類別及對業務影響程度，區分資安全事件等級。

(三)必要時系統管理人員得採取緊急應變措施，防止事件影響擴大。

(四)系統管理人員應記錄事件狀況、應變措施等相關資訊，交由資安聯絡人進行通報。

二、事件通報：

(一)資安聯絡人立即依循內部行政程序，將事件狀況、應變措施等相關資訊向資訊安全長報告。

(二)除單純違反本校校園網路使用規範或其他公約者之外，資安聯絡人應於確認資安事件或接獲校外通知1小時內至「教育機構資安通報平台」登錄事件通報。如因網路或電力中斷無法上網登錄，則應於時限內與區域網路中心及教育機構資安通報應變小組聯繫，先行提供事件細節，俟網路通訊恢復正常後仍須至通報應變網站補登錄通報。

(三)屬3、4級之資安事件，資安聯絡人除上網登錄事件通報外，須另以電話通知區域網路中心及教育機構資安通報應變小組，並提供事件細節內容。

三、事件處理：

(一)系統管理人員進行損害評估，並分析系統復原所需資源。

(二)資安聯絡人協調資通安全處理小組成員進行應變處理作業。

(三)資通安全處理小組依組織、人力、應變措施與所需資源，判定是否自行處理或需請求上級支援。

(四)若判定需請求上級支援，經資訊安全長核定後，應向區域網路中心及教育機構資安通報應變小組提出支援請求。

(五)系統管理人員進行資安事件處理前，應先儲存或備份系統記錄與稽核軌跡等相關資訊，保全事件證據。

(六)系統管理人員應記錄事件處理過程，並填寫「國立嘉義大學資通安全事件處理單」交由事件發生所屬單位進行事件調查，以供後續稽核改善之參考。

四、事件回覆與結案：

(一)資通安全事件處理完成經資訊安全長核定後，資安聯絡人依下列規定時間內回報。

(二)屬3、4級之資安事件，須於確認資安事件36小時內至「教育機構資安通報平台」完成應變流程通報，並向區域網路中心及教育機構資安通報應變小組回報處理結果。若系統無法完成復原應完成損害管制，並尋求業務運作替代方案。

(三)屬1、2級之資安事件，須於確認資安事件72小時內至「教育機構資安通報平台」登錄完成應變流程通報，並完成復原或完成損害管制。

(四)屬0級之資安事件，如為教育部通知疑是侵犯智慧財產權事件，須依教育部規定7天之內回報處理結果。

陸、每年至少應進行一次資通安全事件通報應變演練，並配合於「教育機構資安通報演練平台」登錄演練事件通報。

柒、資通安全事件通報應變作業流程及標準處理程序如附圖。

捌、本作業計畫經計算機諮詢委員會通過，陳請校長核定後實施，並視資安事件應變處理結果或演練成果檢討修正。