# 康寧醫護暨管理專科學校資通安全事件通報應變作業執行要點

民國 97 年 02 月 21 日第 1 次計算機發展委員會會議通過
民國 99 年 11 月 17 日第 2 次計算機發展委員會會議修訂

壹、依據及目的：

一、依據行政院研究發展考核委員會「行政院及所屬各機關資安事件通報應變作業規範(草案)」及本校「康寧醫護暨管理專科學校資訊安全暨緊急應變管理規範」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「康寧醫護暨管理專科學校資通安全事件通報應變作業執行要點」(以下簡稱本要點)。

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，應立即依本要點處理程序辦理。

參、組織及權責：

一、資訊安全長：

由副校長兼任，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) 由本校資訊安全長擔任召集人，資圖中心及本校「計算機發展委員會」委員組成資通安全處理小組，並得委請校內、外學者專家，提供資訊安全顧問諮詢服務及技術支援協助。

(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「國家資通安全通報應變網站」登錄聯絡資料。

(二) 負責對內、對外之資通安全聯繫事宜。

(三) 隨時掌握國家資通安全會報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：

一、『A』級：侵權情節重大者、影響公共安全、社會秩序、人民生命財產。

二、『B』級：系統停頓，業務無法運作。

三、『C』級：系統短暫停頓，業務中斷，短時間可修復。

四、『D』級：系統效能降低，業務遲滯，可立即修復。

五、『E』級：侵權情節輕微者、違反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。

(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，確認為資安事件後，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) 屬『A』、『B』、『C』、『D』級之資安事件，資安聯絡人應於確認資安事件 1 小時內至「國家資通安全通報應變網站」登錄事件通報。如因網路中斷無法上網登錄，則應填具「資訊安全事件通報單」，傳真至國家資通安全會報通報應變組，俟網路恢復後上網登錄補報。

(三) 屬『A』或『B』級之資安事件，資安聯絡人應於確認資安事件 2 小時內向教育部資安聯絡人通報，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，應於確認資安事件 12 小時內向教育部提出申請支援。

(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，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『A』或『B』級之資安事件，須於確認資安事件 **36 小時**內至「國家資通安全通報應變網站」完成通報結案，並向教育部回報處理結果。若系統無法完成恢復應完成損害管制，並尋求業務運作替代方案。

(三) 屬『C』或『D』級之資安事件，須於確認資安事件 **72 小時**內至「國家資通安全通報應變網站」登錄通報事件結案。

(四) 屬『E』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、配合教育部不定期舉辦之資安通報演練，並於資安通報平台完成通報演練。

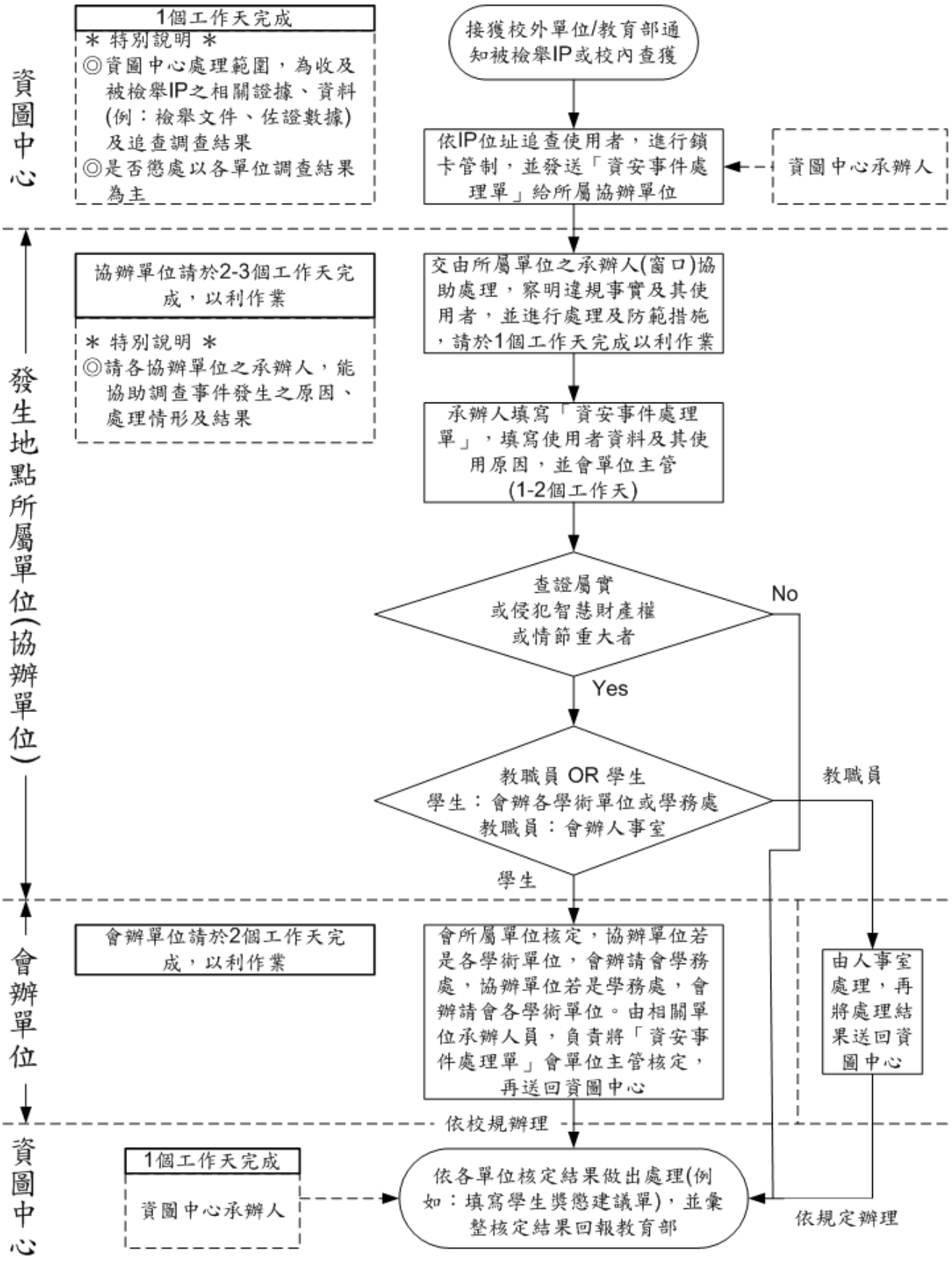
柒、資通安全事件標準處理程序如附圖一，資通安全事件處理單如附表一。

捌、本要點經計算機發展委員會通過，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。

附圖一

# 康寧醫護暨管理專科學校資訊安全事件標準處理程序

※說明：為配合教育部訂定7天內要回報資訊安全處理結果，本校應制定S.O.P.處理流程，以利在時效內回報教育部處理結果，以下為程序圖，希望各單位能在時程內完成。



附表一

# 康寧醫護暨管理專科學校資訊安全事件處理單

**1.資安事件簡述(資圖中心填寫)**

發生日期：____年____月____日　時間：(GMT+0800)_____

IP：_____

發現方式：☐ 校內偵測　☐ 校外單位通知　☐ 教育部通知

事件類別：☐ 針對特定傳輸埠大量掃描

☐ DoS 攻擊，攻擊目標 IP 為_____

☐ 垃圾郵件(SPAM)　☐ 外部攻擊(Attack)　☐ 設備故障：_____

☐ 其他_____

事件說明：_____

_____

影響等級：

☐A級：影響公共安全、社會秩序、人民生命財產。
☐B級：系統停頓，業務無法運作。
☐C級：系統短暫停頓，業務中斷，短時間可修復。
☐D級：系統效能降低，業務遲滯，可立即修復。
☐E級：違反校園網路使用規範或其他公約。(不須通報國家資通安全通報應變網站)

應變措施：☐ 送學務處依校規處理　☐ 停用網路　☐ 停用帳號　☐ 其他_____

協辦單位：_____

聯絡人：_____　資圖中心主任：_____

---

**2.事件調查(協辦單位處理)**

請說明該事件發生之原因和處理情形，以及防範補強措施。

| |
|---|
| |

☐ 處理完畢，不需會辦

承辦人：_____　單位主管：_____

※ 為配合教育部訂定回報資訊安全處理結果之 7 天期限，**處理單位請於___月___日前完成**，以利作業

---

**3.核定(會辦單位處理)**　會辦單位：☐ 學務處　☐ 人事室　☐ 總務處　☐ 其他_____

| |
|---|
| 處理意見： |

承辦人：_____　單位主管：_____

※為配合教育部訂定回報資訊安全處理結果之 7 天期限，**會辦單位請於___月___日前完成**，以利作業