國立政治大學資通安全事件通報及應變處理要點

112 年 03 月 27 日第 19 次資訊安全暨個人資料保護推行委員會會議通過
114 年 11 月 14 日第 24 次資訊安全暨個人資料保護推行委員會會議修正通過

一、為確保國立政治大學（以下簡稱本校）各單位發生資通安全事件時，確實依「資通安全事件通報及應變辦法」（以下簡稱通報及應變辦法）即時通報及應變，降低資通安全事件對本校各單位業務之衝擊影響，特訂定本要點。

二、資通安全事件指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全或保護措施失效之狀態發生，影響資通系統機能運作。

三、本校所有人員發現疑似資通安全事件時，應即時通報，並依本要點或本校電子計算機中心(以下簡稱電算中心)指示，執行後續應變處理事務，提供相關紀錄或資料。

委外廠商發現疑似資通安全事件時，應依契約約定即時通報並為應變處理。

四、資通安全事件之分級及資安預警事件

(一)資通安全事件依「通報及應變辦法」規定分為四級，由輕微至嚴重分別為「1 級」、「2 級」、「3 級」及「4 級」。

(二)如資通系統之機密性、完整性及可用性皆未受影響，以「0 級」表示。

(三)依「臺灣學術網路各級學校資通安全通報應變作業程序」尚未確認是否為資通安全事件者，為資安預警事件。

五、資通安全事件通報流程

(一) 本校所有人員發現疑似資通安全事件者，應立刻通報本校「資通安全事件通報窗口」。

(二) 「資通安全事件通報窗口」接獲通報後，應向權責單位確認；權責單位應配合資安事件調查，並回復資安損害情形。

(三) 「資通安全事件通報窗口」經確認屬資通安全事件後，應於知悉事件 1 小時內至「教育機構資安通報平台」通報登錄資通安全事件細節、影響等級及是否申請支援等資訊。

(四) 如資通安全事件為「3」或「4」級者，電算中心應同時通報資通安全長及上級主管機關，召開會議研商相關事宜，並得請相關機關提供協助。

六、資通安全事件應變流程

資通安全事件之應變處理，包含損害控制及復原、相關紀錄保全、調查、檢討及改善機制。

(一) 損害控制及復原

1. 權責單位應確認具體受害範圍，優先恢復對外服務及核心資通系統運作，防止擴散及次波攻擊，並應依下列規定時間完成損害控制或復原作業：

（1）「1」或「2」級資通安全事件，於知悉事件後 72 小時內。

（2）「3」或「4」級資通安全事件，於知悉事件後 36 小時內。

2. 如無法確認權責單位或發生資通安全事件之系統或設備，為進行損害控制，電算中心得暫時隔離其網路，並透過網站公告。

3. 權責單位應評估各系統於可容忍中斷時間內恢復服務之可能性及對利害關係人之影響，決定是否對外公告事件之相關內容。

(二) 相關紀錄保全、調查

1. 發生資通安全事件，權責單位應留存相關證據資料，並進行適當保護措施，以作為問題分析之依據。

2. 如有釐清事實之必要，電算中心得約談相關人員，如有必要，本校得委請臺灣學術網路危機處理中心或其他外部單位協助調查。

(三) 檢討及改善

1. 資通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，並得修訂相關作業管理規範或建置控制措施。

2. 權責單位應填寫本校「資通安全事件報告單」，說明處理資通安全事件之經過及解決辦法，送交電算中心列管。

3. 電算中心應識別資通安全事件重複發生可能性及影響程度，利用會議、網站或電子郵件等方式，對本校同仁加強宣導，避免類似事件重複發生。

七、重大資通安全事件

「3」或「4」級資通安全事件，屬重大資通安全事件，除依上述規定辦理外，電算中心應依第五點規定通報本校資通安全長及上級主管機關，並依下列規定完成調查、處理及改善。

(一) 經資通安全長同意後，電算中心應成立「資通安全事件調查小組」，成員為權責單位及相關單位之主管或主管指派之人員、電算中心成員、資通安全長指派之資訊安全暨個人資料保護推行委員會委員、學務處或人事室指派之人員。

(二) 於權責單位為初步損害控制後，資通安全長應召集資通安全事件調查小組會議，討論處理重大資通安全事件後續事宜。

(三) 重大資通安全事件涉及個人資料外洩者，依「國立政治大學個人資料保護管理要點」第十八點規定，查明事件後，資料外洩單位應盡速以適當方式通知當事人。

(四) 完成損害控制或復原作業後，權責單位應持續進行資通安全事件之調查及處理，電算中心應於 1 個月內將調查、處理及改善報告提交主管機關。權責單位及電算中心應向「資訊安全暨個人資料保護推行委員會」提出報告。

八、資通安全事件調查結束後，如有違規或違法情事，包含隱匿未進行通報者，得視情形對下列違規或違法之人予以懲處或追究責任：

(一) 為學生者，依「國立政治大學學生獎懲辦法」相關規定辦理。

(二) 為教師者，依「教師法」、「國立政治大學教師評審委員會設置辦法」相關規定辦理。

(三) 為職員者，依「國立政治大學職員獎懲辦法」相關規定辦理。

(四) 為廠商者，本校除得依法舉發或告訴外，並依合約約定辦理。

九、本要點經「資訊安全暨個人資料保護推行委員會」會議通過，校長核定後實施，修正時亦同。