# 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

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」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，依據「資通安全管理法」第 14 條及「國立政治大學資訊安全作業要點」第 38 條訂定本要點。

二、本校所有人員及委外廠商若發現疑似資通安全事件時，皆有即時通報之責任，並應依本要點或本校電算中心指示，執行後續應變處理事務，提供相關紀錄或資料。

三、資通安全事件通報流程

(一) 疑似資通安全事件發生時，發現人員應於知悉事件 1 小時內，通知本校「資通安全事件通報窗口」 (02) 2939 -3091 #63380 或 #67181。

(二) 資通安全事件通報窗口應依「資通安全事件通報及應變辦法」完成資通安全事件等級判斷，並至「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、支援申請等資訊，並確認本次事件權責單位。

(三) 本校自行發現之資通安全事件，權責單位應填具「資通安全事件報告單」針對事件說明解決辦法等處理經過，送交電算中心列管。

(四) 接獲教育機構資安通報平台資通安全事件通報，則依「臺灣學術網路各級學校資通安全通報應變作業程序」之相關流程進行通報。

四、資通安全事件應變流程

本校資通安全應變處理，包含損害控制及復原、相關紀錄保全、調查、檢討及改善機制等步驟。說明如下：

(一) 損害控制及復原

1. 確認具體受害範圍，並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。

2. 評估事件影響，決定是否對外公告事件之相關內容。

3. 完成損害控制或復原作業後，回復本校資通安全事件通報窗口處理情形。

(二) 相關紀錄保全、調查

1. 資通安全事件應留存相關證據資料，並進行適當保護措施，以作為問題分析及法律必要依據。

2. 如有釐清事實之必要，得約談相關人員或委請外部單位協助調查(如臺灣學術網路危機處理中心或檢調單位等)。

(三) 檢討及改善

1. 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。

2. 電算中心應識別資通安全事件重複發生或影響程度，利用會議、網站或電子郵件等方式，對內部同仁加強宣導，避免類似事件重複發生。

五、重大資通安全事件

第三級或第四級資通安全事件，屬重大資通安全事件，除依上述規定辦理外，應立即告知本校資通安全長，並依以下流程完成調查、處理及改善。

(一) 經資通安全長同意後由電算中心成立「資通安全事件調查小組」，成員為事件相關單位、電算中心、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。

(二) 於初步損害控制後，由本校資通安全長召集資通安全事件調查小組會議，討論事件相關事宜。

(三) 涉及個人資料外洩，依本校個人資料保護管理要點第十八條，事件經查明後，由資料外洩單位儘速以適當方式通知當事人。

(四) 完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內將調查、處理及改善報告提交主管機關。且應向「資訊安全暨個人資料保護推行委員會」提出報告。

六、於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，得視情節輕重對人員追究相關責任或予以懲處。

(一) 懲處對象為學生，由所屬系所或學務處簽請予以懲處。

(二) 懲處對象為教職員工，由所屬單位或人事室簽請予以懲處。

(三) 懲處對象為校外人士，函請校外單位協助處理。

七、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。