國立清華大學資通安全事件通報及應變管理程序 (V2.0)

107 學年度第 10 次校務會報紀錄訂定
110 年度第 2 次個人資料保護暨資通安全推動小組管理委員會會議修訂
113 年度第 2 次個人資料保護暨資通安全推動小組管理委員會會議修訂

目錄

壹、 目的

國立清華大學(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校進行通報，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：(03)573-1225、(03)573-1134，聯繫電子郵件信箱為：abuse@cc.nthu.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，應通知本校資通安全事件通報窗口，窗口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全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，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、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長召開會議研商相關事宜，並得請相關機關提供協助與成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全長指派本校之資通安全專責技術人員、資通安全事件通報人員、發生事件之網段網管人員擔任。

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、 通報及應變程序

一、作業程序

(一)如單位或外部人員發現或疑似發生資通安全事件時，發現人員應立刻通報資通安全事件通報窗口，由資通安全事件通報窗口通知「資安事件發生IP」之網段網管人員處理，並副知其單位主管。

(二)如由教育機構資安通報平台或其他資安情資機構通知發現或疑似資通安全事件時，由本校資通安全事件通報窗口通知「資安事件發生 IP」之網段網管人員處理，並副知其單位主管。

(三)本校之權責人員應依據以下事項，於知悉資通安全事件後，依「資通安全事件通報及應變辦法」之規定完成資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。

3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5. 事件其他足以影響資通安全事件等級之因素。

(四)「資安事件發生 IP」之網段網管人員於收到資通安全事件通報窗口通知後，實施應變措施，儘速完成損害控制、復原與事件之調查及處理作業，並將事件發生之事實、可能影響之範圍、損失評估、採取之應變措施等事項，詳細記錄於「資安事件報告單」。

(五)網段網管人員接獲資安通報信件時，請將「資安事件報告單」回復至資通安全事件通報窗口之電子郵件信箱，並副知單位主管。資通安全事件通報窗口應確認「資安事件報告單」填報內容。

(六)本校資安通報窗口於知悉資通安全事件後應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

(七)事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立「緊急處理小組」，立即協助進行處理；接獲本校受託廠商所通報之資通安全事件時，亦同。

(八)本校接獲所屬機關之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核並得依審核結果變更其等級：

1. 通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。

2. 通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。

(九)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資安事件條件成立後 1 小時內，與所隸屬區縣市網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(十)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(十一)本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(十二)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部所指訂或認可之方式，通知該機關。

(十三)本校執行通報應變作業時，得視情形向臺灣學術網路危機處理中心提出

技術支援或其他協助之需求。

二、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

三、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1.資安事件之衝擊及損害控制作業。

2.資安事件所造成損害之復原作業。

3.本校核心及非核心資通系統之資安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。

4.倘涉及個人資料外洩，應評估通知當事人之適當方式，依據本校「PIMS-2-05_個人資料事件之預防、通報及應變程序書」辦理。

5.重大(第「三」級、第「四」級)資安事件應以電子郵件向臺灣學術網路危機處理中心(服務信箱：service@cert.tanet.edu.tw)申請相關鑑識及其他調查作業。

6.重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。

7.重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性之監控。

8.資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。

9.其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委

外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

陸、 重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之主管機關提出前項之報告，以供監督與檢討。

柒、 紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至教育部資訊及科技教育司覆核備查。

二、資通安全事件通報窗口每月應以公文將前一個月之資安事件處理報告呈核至本校資通安全維護計畫執行秘書。

三、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

四、本程序經「資安暨個資管理委員會」通過後施行，修訂時亦同。

捌、 資通安全情資分享與管理

依據本校「資通安全維護計畫第壹拾壹 、資通安全情資之評估及因應」辦理。

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