國立頭城高級家事商業職業學校

資通安全事件通報及應變管理程序

目錄

壹、 目的

國立頭城家商學校(以下簡稱本校)為遵照資通安全管理法第14條、各機關資通安全事件通報及應變處理作業程序(111年10月修正)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部進行通報，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：

(一)聯絡電話：(03)9771131#161

(二)聯絡單位：圖書館資媒組

(三)聯絡人：林格立

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。

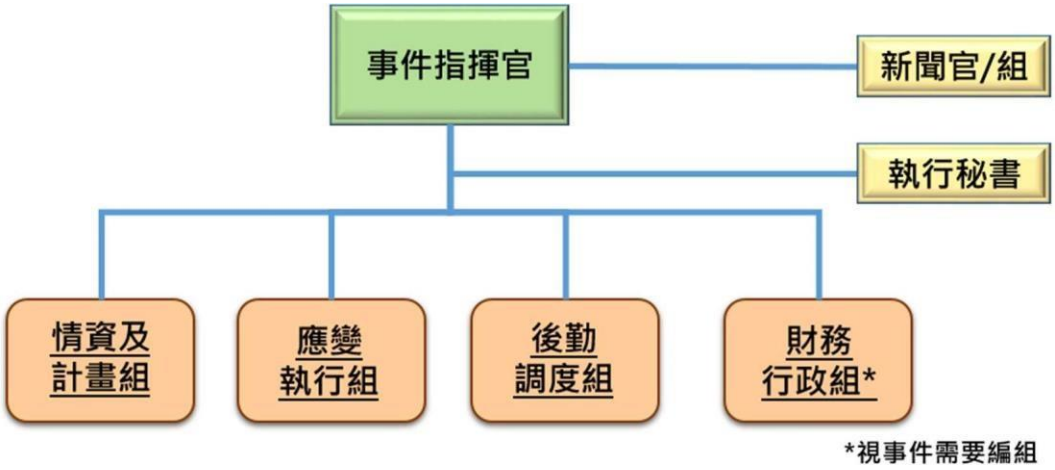
八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬單位或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

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。

十一、各機關應成立資通安全事件通報及應變小組(以下簡稱通報應變小組)，於平時進行演練，並於發生資通安全事件時，依事件等級進行通報及應變作業。

十二、通報應變小組組成建議如圖一，各分組代表如表一，其任務如下：(各小組成員之工作職掌參照「行政院各機關資通安全事件通報及應變處理作業程序」111年修正案。



圖一、資通安全事件通報及應變小組組成

伍、通報作業程序

一、判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

(一). 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

(二). 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。

(三). 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。

(四). 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。

(五). 事件其他足以影響資通安全事件等級之因素。

二、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。

三、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。

四、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。

五、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，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

六、本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

陸、 應變程序

一、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。

二、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. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
4. 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。
5. 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。
6. 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。
7. 其他資通安全事件應變之相關事項。

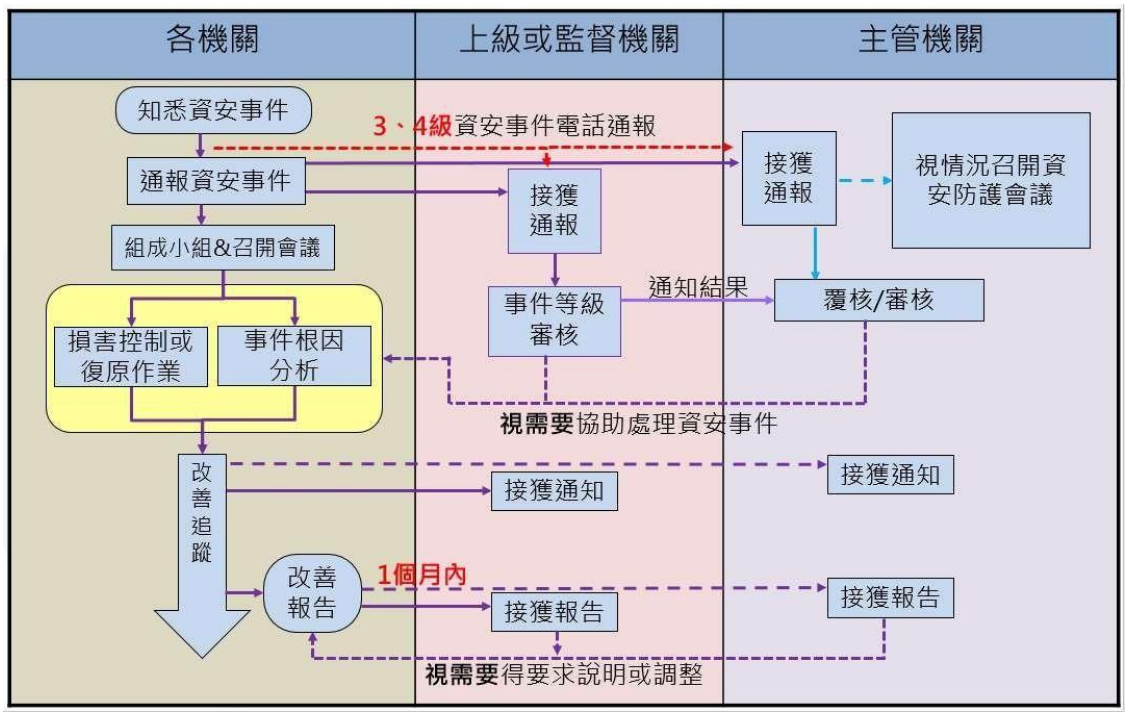
(二) 對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本

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。

（五）整體資安通報程序如下：



柒、 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、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、 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，提交至本部資訊及科技教育司覆核備查。

二、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。

三、需保存之資料如下：

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

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社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院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