嘉義縣中小學資通安全事件通報及應變管理程序

目錄

壹、 目的

嘉義縣立東石國民中學、嘉義縣立大林國民中學、嘉義縣立布袋國民中學、嘉義縣立水上國民中學、嘉義縣立溪口國民中學、嘉義縣立中埔國民中學、嘉義縣立新港國民中學、嘉義縣立民雄國民中學、嘉義縣立六嘉國民中學、嘉義縣立義竹國民中學、嘉義縣立梅山國民中學、嘉義縣立朴子國民中學、嘉義縣立鹿草國民中學、嘉義縣立民和國民中學、嘉義縣立東榮國民中學、嘉義縣立太保國民中學、嘉義縣立過溝國民中學、嘉義縣立忠和國民中學、嘉義縣立嘉新國民中學、嘉義縣立昇平國民中學、嘉義縣立大吉國民中學、嘉義縣立竹崎高級中學、嘉義縣立永慶高級中學、嘉義縣立阿里山國民中小學、嘉義縣立大埔國民中小學、嘉義縣布袋鎮布袋國民小學、嘉義縣布袋鎮景山國民小學、嘉義縣布袋鎮永安國民小學、嘉義縣布袋鎮過溝國民小學、嘉義縣布袋鎮貴林國民小學、嘉義縣布袋鎮新塭國民小學、嘉義縣布袋鎮新岑國民小學、嘉義縣布袋鎮好美國民小學、嘉義縣布袋鎮布新國民小學、嘉義縣大林鎮大林國民小學、嘉義縣大林鎮中林國民小學、嘉義縣大林鎮三和國民小學、嘉義縣大林鎮社團國民小學、嘉義縣大林鎮排路國民小學、嘉義縣大林鎮平林國民小學、嘉義縣民雄鄉民雄國民小學、嘉義縣民雄鄉菁埔國民小學、嘉義縣民雄鄉東榮國民小學、嘉義縣民雄鄉三興國民小學、嘉義縣民雄鄉興中國民小學、嘉義縣民雄鄉秀林國民小學、嘉義縣民雄鄉松山國民小學、嘉義縣民雄鄉大崎國民小學、嘉義縣民雄鄉福樂國民小學、嘉義縣溪口鄉溪口國民小學、嘉義縣溪口鄉美林國民小學、嘉義縣溪口鄉柳溝國民小學、嘉義縣溪口鄉柴林國民小學、嘉義縣新港鄉新港國民小學、嘉義縣新港鄉文昌國民小學、嘉義縣新港鄉月眉國民小學、嘉義縣新港鄉安和國民小學、嘉義縣新港鄉古民國民小學、嘉義縣新港鄉復興國民小學、嘉義縣六腳鄉六腳國民小學、嘉義縣六腳鄉蒜頭國民小學、嘉義縣六腳鄉六美國民小學、嘉義縣六腳鄉北美國民小學、嘉義縣六腳鄉灣內國民小學、嘉義縣六腳鄉更寮國民小學、嘉義縣東石鄉東石國民小學、嘉義縣東石鄉三江國民小學、嘉義縣東石鄉龍港國民小學、嘉義縣東石鄉下楫國民小學、嘉義縣東石鄉港墘國民小學、嘉義縣東石鄉龍崗國民小學、嘉義縣東石鄉網寮國民小學、嘉義縣東石鄉塭港國民小學、嘉義縣義竹鄉義竹國民小學、嘉義縣義竹鄉光榮國民小學、嘉義縣義竹鄉過路國民小學、嘉義縣義竹鄉南興國民小學、嘉義縣義竹鄉和順國民小學、嘉義縣鹿草鄉鹿草國民小學、嘉義縣鹿草鄉重寮國民小學、嘉義縣鹿草鄉下潭國民小學、嘉義縣鹿草鄉竹園國民小學、嘉義縣鹿草鄉後塘國民小學、嘉義縣鹿草鄉碧潭國民小學、嘉義縣水上鄉水上國民小學、嘉義縣水上鄉大崙國民小學、嘉義縣水上鄉柳林國民小學、嘉義縣水上鄉

忠和國民小學、嘉義縣水上鄉義興國民小學、嘉義縣水上鄉成功國民小學、嘉義縣水上鄉南靖國民小學、嘉義縣水上鄉北回國民小學、嘉義縣中埔鄉中埔國民小學、嘉義縣中埔鄉大有國民小學、嘉義縣中埔鄉頂六國民小學、嘉義縣中埔鄉和睦國民小學、嘉義縣中埔鄉同仁國民小學、嘉義縣中埔鄉沄水國民小學、嘉義縣中埔鄉社口國民小學、嘉義縣中埔鄉灣潭國民小學、嘉義縣中埔鄉中山國民小學、嘉義縣中埔鄉和興國民小學、嘉義縣竹崎鄉竹崎國民小學、嘉義縣竹崎鄉龍山國民小學、嘉義縣竹崎鄉鹿滿國民小學、嘉義縣竹崎鄉圓崇國民小學、嘉義縣竹崎鄉內埔國民小學、嘉義縣竹崎鄉桃源國民小學、嘉義縣竹崎鄉中和國民小學、嘉義縣竹崎鄉中興國民小學、嘉義縣竹崎鄉光華國民小學、嘉義縣竹崎鄉義仁國民小學、嘉義縣竹崎鄉沙坑國民小學、嘉義縣梅山鄉梅山國民小學、嘉義縣梅山鄉梅圳國民小學、嘉義縣梅山鄉太平國民小學、嘉義縣梅山鄉太興國民小學、嘉義縣梅山鄉瑞里國民小學、嘉義縣梅山鄉瑞峰國民小學、嘉義縣梅山鄉大南國民小學、嘉義縣梅山鄉太和國民小學、嘉義縣梅山鄉仁和國民小學、嘉義縣梅山鄉梅北國民小學、嘉義縣番路鄉民和國民小學、嘉義縣番路鄉內甕國民小學、嘉義縣番路鄉黎明國民小學、嘉義縣番路鄉大湖國民小學、嘉義縣番路鄉隙頂國民小學、嘉義縣阿里山鄉香林國民小學、嘉義縣阿里山鄉十字國民小學、嘉義縣阿里山鄉達邦國民小學、嘉義縣阿里山鄉山美國民小學、嘉義縣阿里山鄉新美國民小學、嘉義縣阿里山鄉來吉國民小學、嘉義縣阿里山鄉茶山國民小學、嘉義縣豐山實驗教育學校、嘉義縣太保市太保國民小學、嘉義縣太保市安東國民小學、嘉義縣太保市南新國民小學、嘉義縣太保市新埤國民小學、嘉義縣朴子市朴子國民小學、嘉義縣朴子市雙溪國民小學、嘉義縣朴子市大同國民小學、嘉義縣朴子市竹村國民小學、嘉義縣朴子市松梅國民小學、嘉義縣朴子市大鄉國民小學、嘉義縣朴子市祥和國民小學(以下簡稱各校)為遵照資通安全管理法第 14 條及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

發生於各校之事件，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、各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、各校應視必要性，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該校進行通報，於完成事件之通報及應變程序後，依該校指示提供相關之紀錄或資料。

三、各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、各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、各校之資通安全事件通報窗口及聯繫專線為：嘉義縣教育網路中心，05-2304464。

四、各校應以適當方式使相關人員明確知悉該校之通報窗口及聯絡方式。

五、各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、各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；接獲該校所屬分校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各校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。

伍、 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

各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：

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。

(二)各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，各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)各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)各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)各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

各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，應依據該校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，各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，各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)各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)各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。

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、各校若發生重大(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、各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、各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、各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。

玖、 演練作業

一、各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、各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