國立大湖高級農工職業學校資通安全事件通報及應變處理作業程序

111年10月11日國立大湖農工**資通安全管理審查會議通過**
111年10月17日湖農工圖字第1110008271號公告施行

一、國立大湖高級農工職業學校(以下簡稱本校)為確保於發生資通安全事件時，依資通安全管理法(以下簡稱本法)及資通安全事件通報及應變辦法相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對本部業務之衝擊影響，並確保資通安全事件發生時之跡證保存，特訂定本作業程序。

二、本校資通安全事件通報及應變小組(以下簡稱通報應變小組)組成如附件一，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。通報應變小組各分組代表如附件二，其任務如下：

(一)事件指揮官：為通報應變小組總召集人，綜理全般業務，直接督導各單位聯絡人員及新聞發言人。

(二)新聞發言人：為資通安全事件對外發布新聞或說明之單一窗口，負責綜整與定期更新訊息。

(三)執行秘書：為事件指揮官幕僚，負責督辦通報及應變小組各項業務。

(四)情資及計畫組：

1.本分組負責辦理下列事宜：

(1)資通安全事件通報及情資分享：透過資通安全監控中心(SOC)、防毒軟體及系統釐清事件影響，並清查各單位受影響情形，據以完成資通安全事件各階段通報，分享惡意程式 IoC(Indicators of Compromise)等。

(2)應變策略及計畫研擬：於發生重大資通安全事件時，依據事件情況研擬損害控制、復原作業及跡證保存計畫。

2.本分組由本校資通安全專職人員、資訊人員、業務單位及委外廠商或外部專家組成。

(五)應變執行組：

1.本分組負責辦理下列事宜：

(1)執行損害控制：依據情資及計畫組研擬之應變策略及計畫，調度人員執行災害搶救及損害管制，防止次波攻擊及損害擴散。

(2)復原作業：依據情資及計畫組研擬之復原作業，完成系統重建、弱點掃描或漏洞修補等事宜。

(3)跡證保全及留存：確保受害系統與相關系統及網路設備事件日誌之保存及管理。

2. 本分組由本校資通安全專職人員、資訊人員、業務單位及委外廠商或外部專家組成。

(六)後勤調度組：

1.本分組負責辦理下列事宜：

(1)事件根因查找：依據系統保存跡證，完成鑑識分析，並追查防堵惡

意中繼站。

(2) 提出改善建議：依據事件調查根因，提出短、中、長期改善建議。

(3) 彙整改善報告。

(4) 撰寫調查、處理及改善報告。

(5) 追蹤管考:針對機關單位已結案或未結案事項,如有未盡改善事宜，將另案追蹤管考。

2. 本分組由本校資通安全專職人員、資訊人員、業務單位及委外廠商或外部專家組成。

(七) 財務行政組：

本分組視事件需要由主計單位組成,負責辦理預算調撥及提供行政支援事宜。

三、 資通安全事件通報及應變程序應包含通報資通安全事件、召開事件應變會議、損害控制或復原作業、事件根因分析及改善追蹤等項目（如附件三)，並依本法施行細則第六條第一項第九款規定納入資通安全維護計畫中。

前項各程序如下：

(一)通報資通安全事件：

1. 本校應依本法及資通安全事件通報及應變辦法規定，由情資及計畫組依國教署指定方式完成事件通報，並於本校即時通訊群組通知相關事件處理人員。

2. 第三級或第四級資通安全事件除依前目規定辦理外；另須填寫「**資通安全事件通報/處理速報單**」(如附件四)陳報國教署。

(二) 召開事件應變會議:第三級或第四級資通安全事件應於完成初步損害控制後，召開事件應變會議，會議形式不拘，由事件指揮官主持討論下列事項

1. 資通安全事件概況。

2. 評估受影響範圍。

3. 其他必要之討論事項。

(三) 損害控制或復原作業：

1. 由應變執行組執行損害控制或復原作業，並辦理下列事項：

(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，防止次波攻擊及擴散情形。

(2) 評估各系統是否於可容忍中斷時間內恢復服務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。

(3) 於完成損害控制或復原作業後，依國教署指定之方式完成通知作業。

2. 第三級或第四級資通安全事件，除依前目規定辦理外，並應辦理下列事項：

(1) 定時向事件指揮官、通報及應變小組成員及國教署回報控制措施成效。

(2) 倘涉及個人資料外洩，應依個人資料保護法第十二條規定及相關規

定辦理。

（四）事件根因分析：由應變執行組執行事件根因分析，辦理事項如下：

1. 依第四點規定辦理跡證保存時，如發現惡意程式，應上傳至 Virus Check 網站（https://viruscheck.tw/）進行檢測；因故無法上傳時，應送交防毒軟體或資安服務公司檢測。

2. 除設備故障外，應依第四點規定辦理跡證保存，並由組長督導委外廠商或外部專家進行根因調查，提出紀錄分析；如有發現惡意程式，應提出惡意程式分析。

3. 依據事件調查報告，應評估短、中、長期資安管理改善策略，其內容如下：

（1）短期：完成可立即性修補項目之調整，例如更換密碼或修補程式弱點等。

（2）中期：依據事件根因提出三個月至六個月內完成之強化作為，例如盤點老舊設備，並訂定汰換期程。

（3）長期:依據事件受害情形,視需要提出二年內完成之管理改善建議，例如培養本校資安人員能力等。

4. 第三級或第四級資通安全事件，由執行秘書將事件調查根因及改善策略提報事件指揮官核定，並由資通安全專職人員彙整送交國教署。

（五）改善追蹤：由應變執行組進行事件改善追蹤時，應辦理下列事項：

1. 評估改善作為期程。

2. 評估執行成效，並據以調整改善策略。

3. 配合國教署辦理相關改善作為。

4. 由執行秘書將各階段改善措施執行成效定期回報事件指揮官至完成各項改善措施為止，並由資通安全專職人員彙整送交國教署。

5. 依指定之方式，送交調查、處理及改善報告；第三級或第四級資通安全事件，應另以密件公文將該報告送交國教署。

6. 本校送交調查、處理及改善報告後，相關改善事項應納入定期追蹤管考機制。

四、為確保資通安全事件發生時，所保有跡證足以進行事件根因分析，應辦理下列事項，並應視事件情形辦理其他必要之跡證保存事項：

（一）於日常維運資通系統時，應依附件五保存日誌（log ），並定期備份於外部設備或媒體。

（二）發生資通安全事件時，應依下列原則進行跡證保存：

1. 進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。

2. 若系統無備援機制，應備份受害系統儲存媒介（例如硬碟、虛擬機映像檔）後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。

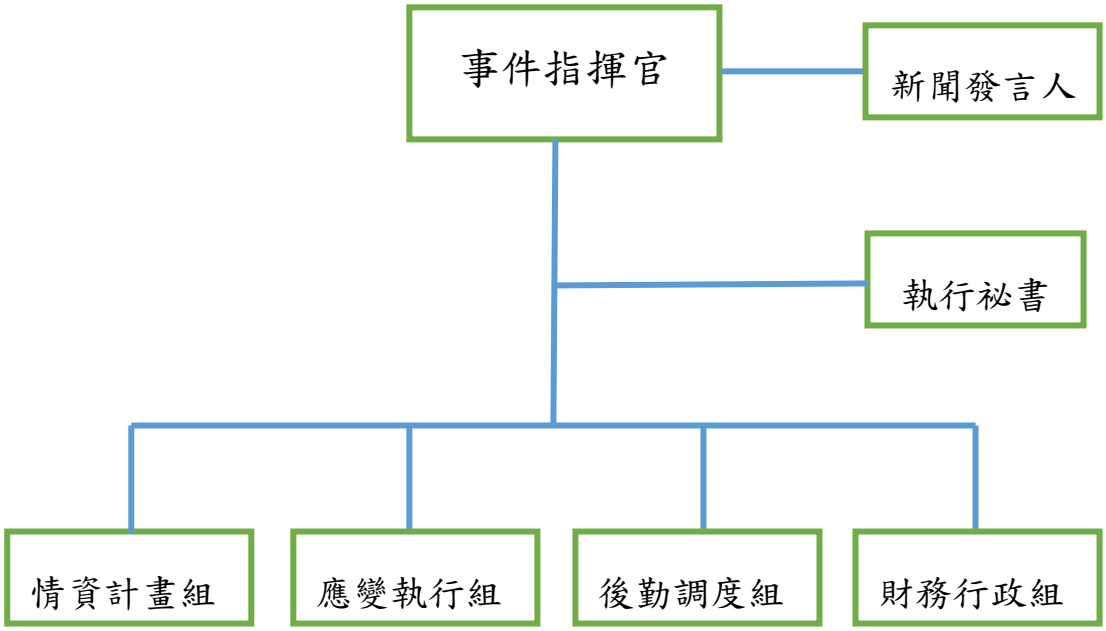
3. 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害

系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。

4. 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。

（三）於簽訂資通系統或服務之委外契約時，應依前二款規定於契約中定明紀錄保存及備份規定。

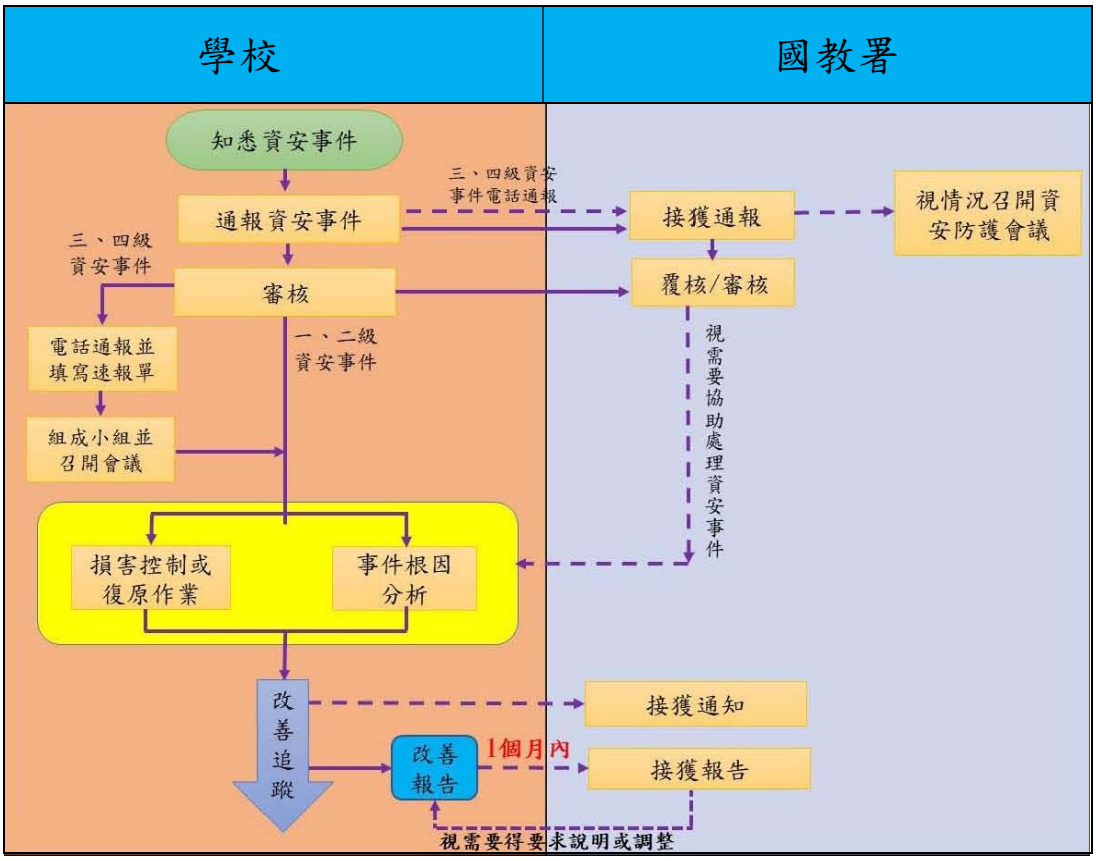
附件一　資通安全事件通報及應變小組組成



附件二　資通安全事件通報及應變小組各分組代表

	第一級、第二級資通安全事件	第三級、第四級資通安全事件
事件指揮官	資安長(教務主任)	校長
新聞發言人	秘書	秘書
執行秘書	圖書館主任	圖書館主任
情資計畫組	圖書館主任	圖書館主任
應變執行組	設備組長	教務主任
後勤調度組	兼任資安人員	總務主任
財務行政組	主計主任	主計主任

附件三　資通安全事件通報及應變程序



附件四

資通安全事件通報/處理速報單

<table>
<tr><td colspan="3">通報人姓名：　　通報單位：
事件發生點：　　通報時間：　　年　　月　　日　　時　　分</td></tr>
<tr><td colspan="2">事件分類
□非法入侵　□感染病毒　□阻斷服務
□系統當機　□實體毀損　□資料遭竊
□資料庫毀損□網頁遭篡改□其他_____</td><td>事件說明</td></tr>
<tr><td colspan="3">原因分析</td></tr>
<tr><td colspan="3">可能影響範圍或損失
□電腦機房 □對外線路 □內部網路 □業務_____□其他_____</td></tr>
<tr><td colspan="3">資安事件等級： □ 4 級事件 □ 3 級事件 □ 2 級事件 □ 1 級事件</td></tr>
<tr><td colspan="2" rowspan="2">矯正措施：

預計完成日期：__/__/__</td><td>資安事件處理人</td></tr>
<tr><td>資安長</td></tr>
</table>

事件通報紀錄

是否通報本校資訊安全長？

□是(時間___/___/__ __:__ 通報人簽名:_____) □不需

是否通報機關單位主管？

□是(時間___/___/__ __:__ 通報人簽名:_____) □不需

是否通報國家資通安全通報應變網站？

□是(時間___/___/__ __:__ 通報人簽名:_____) □不需

處理追蹤紀錄 □詳見查核註記

查核註記(請填寫查核內容、未完成原因說明、查核時間、查核人等資訊)

結案確認	資安事件處理人	單位主管	校長

(一) 4 級事件

符合下列任一情形者，屬 4 級事件：

1. 國家機密資料遭洩漏。
2. 關鍵資訊基礎設施系統或資料遭嚴重竄改。
3. 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

(二) 3 級事件

符合下列任一情形者，屬 3 級事件：

1. 密級或敏感資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改。

3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

（三）2 級事件

符合下列任一情形者，屬 2 級事件：

1. 核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。
2. 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改。
3. 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

（四）1 級事件

符合下列任一情形者，屬 1 級事件：

1. 非核心業務一般資料遭洩漏。
2. 非核心業務系統或資料遭輕微竄改。
3. 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

(五)事件通報窗口及緊急處理小組

1. 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：

   (1) 聯絡電話：(07)525-0211

   (2) 網路電話：98400000

   (3) 電子郵件：service@cert.tanet.edu.tw

2. 教育部 國民及學前教育署 高級中等教育組

   (1) 連絡電話：(04)3706-1123

   (2) 電子郵件：e-2131@mail.k12ea.gov.tw

3. 教育部 國民及學前教育署 國立高級中等以下學校 DNS、學校網頁向上集中計畫 成大維運團隊

   (1) 連絡電話：(06)2761-271

   (2) 電子郵件：dnsweb@hs.edu.tw

本校之資通安全事件通報窗口及聯繫專線為：

(一)　聯絡電話：(037)992216-710

(二)　電子郵件：khr003@mail.edu.tw

4. 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。
5. 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。

附件五　　日誌保存範圍及項目

保存範圍	保存項目
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)