苗栗縣立三灣國中資安事件通報規定

作業程序說明

一、資訊安全事件之管理

(一) 應建立資訊安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速、有效處理資訊安全事件。

(二) 資訊安全事件之處理程序，應視需要納入下列事項：

1. 導致資訊安全事件原因之分析。
2. 防止類似事件再發生之補救措施。
3. 電腦稽核軌跡及相關證據之蒐集。
4. 與受影響之使用者進行溝通及說明。

(三) 電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

1. 作為研析問題之依據。
2. 作為研析是否違反契約或資訊安全規定之證據。
3. 作為與委外廠商協商如何補償之參考。

(四) 應依據「資訊安全事件通報與應變作業流程圖」處理資訊安全事件。相關作業程序應考量下列事項：

1. 考量單位資源，於最短的時間內，確認復原後之系統及相關安全控制是否完整及正確。
2. 向管理階層報告處理情形，並檢討、分析資訊安全事件。
3. 限定僅授權之人員可使用回復後正常作業之系統及資料。
4. 緊急處理步驟應詳實記載，以備日後查考。

二、通報程序

(一) 疑似資訊安全事件發生時，發現人員應依事件歸屬通報權責單位，並副知直屬主管。

(二) 權責單位於收到通知後，研判是否為資訊安全事件。若：

1. 判定為非資訊安全事件時，則將結果回覆予發現人員。
2. 判定為資訊安全事件時，初估事件處理時間，並報告中心主任。
3. 資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。

(1). 4 級事件，符合下列任一情形者：

A. 國家機密資料遭洩漏。

B. 國家重要資訊基礎建設系統或資料遭竄改。

C. 國家重要資訊基礎建設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。

(2). 3 級事件，符合下列任一情形者：

A. 密級或敏感公務資料遭洩漏。

B. 核心業務系統或資料遭嚴重竄改。

C. 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。

(3). 2 級事件，符合下列任一情形者：

A. 非屬密級或敏感之核心業務資料遭洩漏。

B. 核心業務系統或資料遭輕微竄改。

C. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

(4). 1 級事件，符合下列任一情形者：

A. 非核心業務資料遭洩漏。

B. 非核心業務系統或資料遭竄改。

C. 非核心業務運作遭影響或短暫停頓。

(三) 發現人員應於確認資訊安全事件後，填寫「資訊安全事件報告單」，交本中心權責單位處理。

(四) 決策處理：

1. 當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時，由權責單位自行處理，並將處理後狀況通知各組組長或中心主任。

2. 事件處理過程中如發現所造成之影響大於原先判定時，權責單位應立即向中心主任報告，並重新執行事件分析及辨識。

3. 應參考『教育機構資安通報應變手冊』之通報與應變作業流程，並依據事件影響等級，向教育部通報。

(五) 有關是否啟動業務永續運作計畫，依「業務永續運作管理程序書」辦理。

三、危機處理程序

(一) 本中心資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

1. 事前建置安全防護機制：

(1). 建置資訊安全管理系統及整體防護架構。

(2). 彙整及備妥資訊安全相關文件。

2. 事中主動預警與緊急應變：

(1). 事件辨識：辨識事件之歸屬及採取之對策，如：內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。

(2). 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

(3). 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向「資訊安全工作組」提出建議方案。

(4). 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

3. 事後復原追蹤鑑識偵查：

(1). 後續事件追蹤以避免及降低類似資訊安全事件重複發生機率，並檢視現有環境安全漏洞，經由研析相關資料，以釐清事件發生之原因與責任。

(2). 受損單位依復原程序實施災後復原重建。

(3). 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務中心或警調單位申請數位鑑識（電腦、網路鑑識）。

(4). 若重大事件危及人員生命安全，則應通報國家災害防救體系。

苗栗縣立三灣國中資安事件通報規定

四、檢討及改善

(一) 資訊安全事件確認處理完成後，權責單位應檢討現行管控措施之完整性，並適當修訂相關作業規範或建置及調整控制措施，必要時應召開檢討會議。

(二) 權責單位應依「矯正及預防管理程序書」規定處理採取必要之矯正及預防措施，以避免類似安全事件重複發生。

控制重點

一、機關於發生資安事件時，是否依通報作業程序，於規定的期限內，至「教育機構資安通報平台」通報登錄資安事件(https://info.cert.tanet.edu.tw)。

二、機關於發生資安事件時，是否於規定的期限內，進行損害管制。

三、機關是否訂定災害預防、緊急應變程序、復原計畫等防護措施，並定期演練。

四、機關是否針對機敏文件、資料及檔案等，採取加密或實體隔離等防護措施。

五、機關是否執行入侵偵測、安全掃描及弱點檢測等安全檢測工作。

六、機關是否於每半年實施內部稽核 1 次。

七、機關是否於發生資安事件時，依訂定之緊急應變計畫，實施緊急應變處置。

八、機關是否於資安事件結束後，彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並檢討應變作業。

九、機關於資安事件處理後，是否至「教育機構資安通報平台」通報結案。

法令依據

一、教育部「教育機構資安通報應變手冊」

二、教育體系資通安全管理規範

三、本校資訊科技中心「安全事件管理程序書」

四、本校資訊科技中心「業務永續運作管理程序書」

五、本校資訊科技中心「矯正及預防管理程序書」

六、本校資訊科技中心「資訊安全事件通報與應變作業流程圖」