國立玉里高級中學

安全事件管理程序書

機密等級：一般

文件編號：**YLSH-B-011**

版　　次：**1.0**

發行日期：**109.10.23**

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

安全事件管理程序書					
文件編號	YLSH-B-011	機密等級	一般	版次	1.0

目錄

安全事件管理程序書					
文件編號	YLSH-B-011	機密等級	一般	版次	1.0

1 目的

建立國立玉里高級中學（以下簡稱「本校」）資通安全事件處理程序，降低事件所造成之損害，從而建立事件學習機制，以識別重複發生之資通安全事件。

2 適用範圍

本校承辦相關資訊業務之資通安全事件管理。

3 權責

3.1 資通安全委員會：審核本校「資通安全事件通報與應變作業流程」，並督導資通安全事件之管理作業。

3.2 資通安全小組：研擬資通安全事件通報流程。

3.3 發現人員：所有人員（含：本校人員、約聘[僱]人員及工讀生與委外駐點人員），發現疑似資通安全事件時，皆負有即時通報之責任。

3.4 權責單位：資通安全事件處理之權責單位，須執行資通安全事件之分析及處理。

3.5 資通安全執行祕書：督導資通安全事件通報、處理及分析作業。

3.6 緊急處理小組：

3.6.1 確定事件影響範圍，並評估損失。

3.6.2 協助資通安全事件之通報、處理及分析作業。

3.7 支援單位：

3.7.1 本校內部單位：協助處理相關法律、人事懲處及採購等問題。

3.7.2 委外廠商：協助處理資通安全事件。

4 名詞定義

4.1 資通安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

4.2 內部資安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎等事件。

4.3 外力入侵事件：發現（或疑似）電腦病毒感染事件、駭客攻擊（或非法入侵）等事件。

4.4 天然災害：颱風、水災、地震等。

4.5 突發事件：火災、爆炸、重大建築災害及資訊網路系統骨幹（主幹寬頻）中斷事件等。

5 作業說明

5.1 資通安全事件之管理

5.1.1 應建立資通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通安全事件。

5.1.2 除正常應變計畫（如：系統及服務之回復作業），資通安全事件之處理程序，應視需要納入下列事項：

5.1.2.1 導致資通安全事件原因之分析。

5.1.2.2 防止類似事件再發生之補救措施。

5.1.2.3 電腦稽核軌跡及相關證據之蒐集。

5.1.2.4 與受影響之使用者進行溝通及說明。

5.1.3 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：

5.1.3.1 作為研析問題之依據。

5.1.3.2 作為研析是否違反契約或資通安全規定之證據。

5.1.3.3 作為與委外廠商協商如何補償之依據。

5.1.4 應依據「資通安全事件通報與應變作業流程」處理資通安全事件。相關作業程序應注意下列事項：

5.1.4.1 考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

5.1.4.2 向管理階層報告處理情形，並檢討、分析資通安全事件。

5.1.4.3 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.1.4.4 緊急處理步驟應詳實記載，以備日後查考。

5.2 通報程序

5.2.1 疑似資通安全事件發生時，發現人員應依事件歸屬通報權責單位，並通知直屬主管。

5.2.2 權責單位於收到通知後，研判是否為資通安全事件。若：

5.2.2.1 判定為非資通安全事件時，則將結果回覆予發現人員。

5.2.2.2 判定為資通安全事件時，初估事件處理時間，並通知資通安全官。

5.2.2.3 資通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」。

5.2.2.3.1 4 級事件，符合下列任一情形者：

5.2.2.3.1.1 機密資料遭洩漏。

5.2.2.3.1.2 關鍵業務系統或資料遭嚴重竄改。

5.2.2.3.1.3 關鍵業務系統運作停頓，無法於可容忍中斷時間內回復正常運作。

5.2.2.3.2 3 級事件，符合下列任一情形者：

5.2.2.3.2.1 敏感資料遭洩漏。

5.2.2.3.2.2 關鍵業務系統或資料遭竄改。

5.2.2.3.2.3 關鍵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。

5.2.2.3.3 2 級事件，符合下列任一情形者：

5.2.2.3.3.1 限閱等級資料之關鍵業務系統或資料遭洩漏。

5.2.2.3.3.2 關鍵業務系統或資料遭輕微竄改。

5.2.2.3.3.3 關鍵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。

5.2.2.3.4 1 級事件，符合下列任一情形者：

5.2.2.3.4.1 非關鍵業務系統或資料遭洩漏。

5.2.2.3.4.2 非關鍵業務系統或資料遭竄改。

5.2.2.3.4.3 非關鍵業務運作遭影響或短暫停頓可立即修復。

5.2.3 權責單位於發生資通安全事件時，應立即填具「資通安全事件報告單」。

5.2.4 決策處理：

5.2.4.1 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（如：電腦病毒感染），由權責單位自行處理，並將處理後狀況通知單位主管及資通安全官。

5.2.4.2 處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資通安全官報告，重新執行事件分析辨識。

5.2.4.3 資通安全執行祕書應參考『臺灣學術網路各級學校資通安全通報應變作業程序』，並依據權責單位所提報之事件影響報告，決定是否向上級主管單位通報。若需要通報，應由單位主管確認後執行。

5.2.5 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。

5.3 危機處理程序

5.3.1 本校資通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：

5.3.1.1 事前建置安全防護機制：

5.3.1.1.1 建置資通安全管理系統及整體防護架構。

5.3.1.1.2 彙整及備妥資通安全相關文件。

5.3.1.2 事中主動預警與緊急應變：

5.3.1.2.1 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。

5.3.1.2.2 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。

5.3.1.2.3 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，應向資通安全委員會提出建議方案。

5.3.1.2.4 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。

5.3.1.3 事後復原追蹤鑑識偵查：

5.3.1.3.1 後續追蹤之精神乃係檢討相關資通安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

5.3.1.3.2 受損單位依復原程序實施災後復原重建。

5.3.1.3.3 重大資通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檢警單位申請數位鑑識（電腦、網路鑑識）。

5.4 檢討及改善

5.4.1 安全事件確認處理完成後，權責單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施。必要時，應召開檢討會議。

5.4.2 權責單位應依「矯正及預防管理程序書」規定處理，以避免類似安全事件重複發生。

5.5 從資訊安全事故中學習

5.5.1組織應由資訊安全事故所得的資訊,識別其重複發生或其影響程度,利用會議、內部網站或電子郵件等方式,對組織內員工加強宣導,避免事故重覆發生。

5.5.2資安事件若由本校教職員、生不當行為造成,得依照教育部頒訂之「臺灣學術網路使用規範」、本校「校園網路管理辦法」及其他相關法令法規之規定辦理。

5.6 證據的收集

5.6.1為預防資安事故發生後,若需做為民事或刑事訴訟事件的相關鑑識證據,例如:遵照電腦誤用或資料保護法。組織應將事故發生過程中的相關紀錄或資料保存。

5.6.2資安事件發生後,組織內為了處置懲處行動之目的而收集和呈現證據時,證據收集法則應涵蓋:

5.6.2.1 證據的可採用性:此項證據是否可以在法庭上使用。

5.6.2.2 證據的證據力(weight):證據的品質與完全性。為達到證據的可採用性,組織宜確保其資訊系統遵循可採用證據產生方法的相關已公告標準或作業規範。

5.6.3組織可根據以下條件建立有力的證據存底:

5.6.3.1 紙本文件:記錄發現者、發現地點、發現時間及發現時在場證人的原始文件要妥為保管,任何調查都宜確保原始文件未遭竄改。

5.6.3.2 關於電腦媒體上的資訊:所有可移除式媒體、硬碟上或記憶體中的資訊宜製作鏡像(mirror image)或複本(依適用要求),以確保可用性;複製過程的所有活動宜保留日誌,且過程宜有見證;宜以安全方式保持原始媒體與日誌(若不可能,至少一份鏡像或複本),並使其不被變動。

5.7 資訊安全事件證據資訊的保護

5.7.1所有鑑識工作只宜在證據資訊的複本上執行。

5.7.2應保護所有證據材料的完整性。

5.7.3證據資訊的複製宜由值得信賴的人員監督，執行複製過程的時間、地點、執行複製活動的人員、利用的工具和程式等資訊應予以存錄。

6 相關文件

6.1 臺灣學術網路各級學校資通安全通報應變作業程序

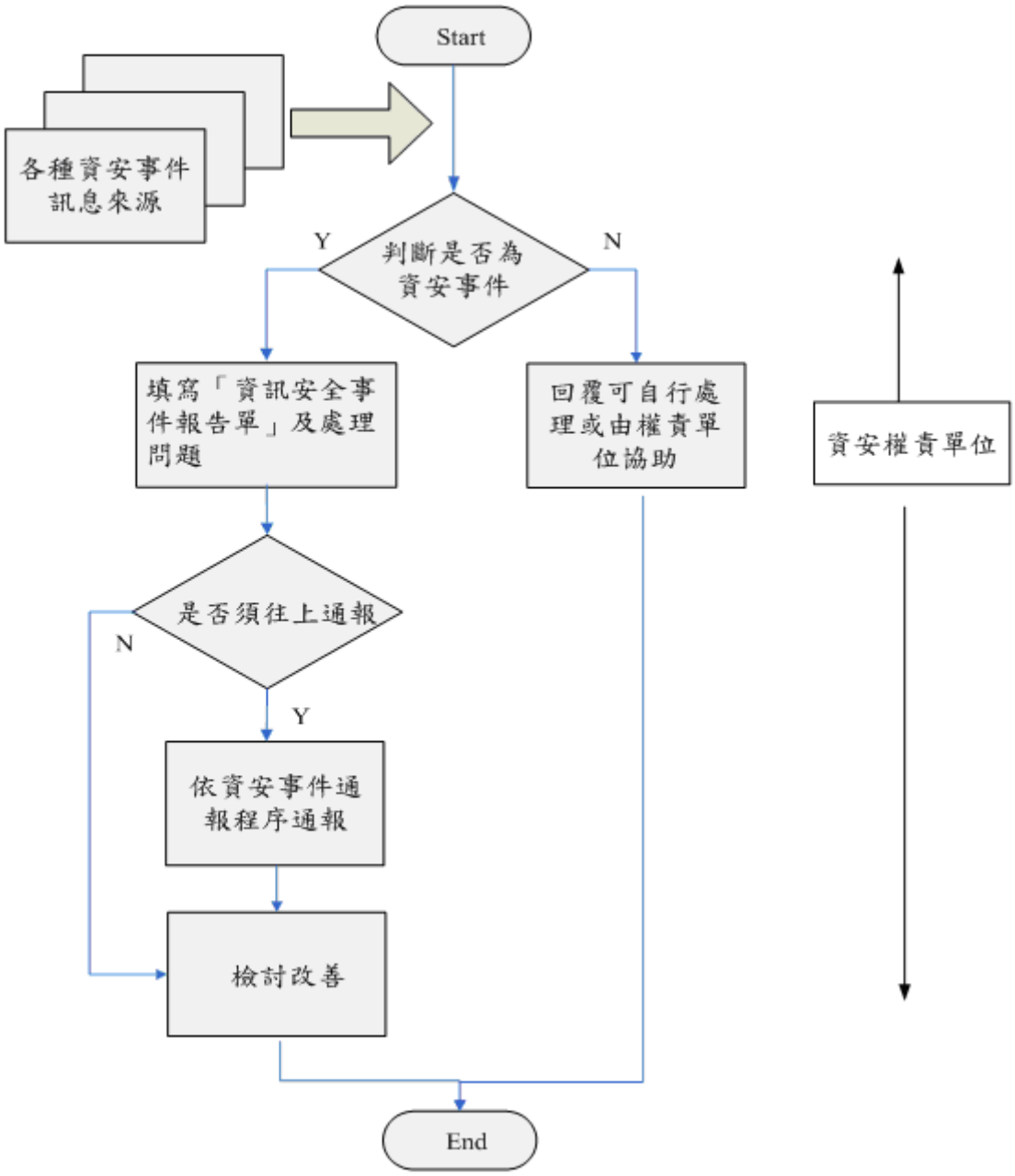
6.2 業務永續運作管理程序書

6.3 矯正及預防管理程序書

6.4 資通安全事件報告單

7 附件

7.1 資通安全事件通報與應變作業流程


Start
各種資安事件訊息來源
判斷是否為資安事件
Y
N
填寫「資訊安全事件報告單」及處理問題
回覆可自行處理或由權責單位協助
資安權責單位
是否須往上通報
N
Y
依資安事件通報程序通報
檢討改善
End