保西國小資安通報處理程序

1　目的

確保保西國小（以下簡稱本校）於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

2　適用範圍

本校施作範圍內資訊業務之資訊安全事件管理。

3　權責

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

3.2　資訊安全小組：研擬資訊安全事件通報流程。

3.3　發現人員：所有人員（含：本校人員、約聘僱人員與委外駐點人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

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

3.5　資訊安全官：督導資訊安全事件通報、處理及分析作業。

3.6　緊急處理組：

3.6.1確定事件影響範圍，並評估損失。

3.6.2協助資訊安全事件之通報、處理及分析作業。

3.7　支援單位：

3.7.1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：協助處理資訊安全事件。

4 名詞定義

4.1 資訊安全事件：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 內部危安事件：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 資訊安全事件之管理

5.1.1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。

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

5.1.2.1 導致資訊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訊安全規定之證據。

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「資訊安全事件通報與應變作業流程」處理資訊安全事件。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、分析資訊安全事件。

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，並副本告知直屬主管。

5.2.2權責單位於收到通知後，研判是否為資訊安全事件。若：

5.2.2.1 判定為非資訊安全事件時，則將結果回覆予發現人員。

5.2.2.2 判定為資訊安全事件時，初估事件處理時間，並通知資訊安全官。

5.2.2.3 資訊安全事件等級區分為：

5.2.2.3.1 A 級：影響校園安全及秩序。

5.2.2.3.2 B 級：系統停頓，業務無法運作。

5.2.2.3.3 C 級：業務中斷，影響系統效率。

5.2.2.3.4 D 級：業務短暫停頓，可立即修復。

5.2.3權責單位於發生資訊安全事件時，應立即填具「資訊安全事件報告單」。

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訊安全官。

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訊安全官報告，重新執行事件分析辨識。

5.2.4.3 資訊安全官應參考『國家資通安全會報通報與應變作業流程』，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：

5.3.1.1 事前建置安全防護機制：

5.3.1.1.1 建置資訊安全管理系統及整體防護架構。

5.3.1.1.2 彙整及備妥資訊安全相關文件。

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，應向資訊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訊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單位或檢警單位申請數位鑑識（電腦、網路鑑識）。

6 相關文件

6.1 業務永續運作管理程序書

6.2 資訊安全事件通報與應變作業流程

6.3 資訊安全事件報告單