管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-009	
文件名稱	資訊安全事件管理程序書	
發行單位	文件管制小組	
發行日期	104年07月06日	
版　　次	A	
訂修廢單位	審　　查	核　　准
資通安全處理小組	資訊發展中心 中心主任 陳君毓	行政副校長 翁順祥

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
A	104/07/06	初版發行

1. 目的

1.1. 為使本校資訊安全事件之處理有一明確之規範，將安全及失效事件所造成的損害降到最低，並且建立事件學習機制，以識別重複發生的安全或失效事件。

1.2. 確保本校於資訊安全事件發生時，能迅速依通報程序進行通報，並採取必要之應變措施，降低事件可能帶來之衝擊與損害。

2. 適用範圍

凡本校與資訊安全相關作業環境中之資訊安全事件，均適用本程序書。

3. 參考文件

3.1. ISMS-P-006 業務持續管理程序書。

3.2. ISMS-W-004 軟硬體故障緊急應變作業標準書。

3.3. ISMS-W-005 網路連線中斷緊急應變作業標準書。

3.4. ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

4.1. 資訊安全事件：凡於資訊作業環境中，資訊或資訊系統之機密性、完整性、可用性遭受破壞之事件。

4.2. 發現人員：指所有人員含正式員工與非正式員工（臨時員工或第三方派駐本校人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

5. 作業內容

5.1. 資訊安全事件通報及危機處理流程圖

作業流程	權責單位	相關表單
發現資安事件	發現人員	資訊安全事件報告單
發出通報	資通安全處理小組	資訊安全事件報告單
執行各項危機處理	資通安全處理小組	資訊安全事件報告單
評估（No：回執行各項危機處理）	依等級判別評估人員	資訊安全事件報告單 資訊安全事件報告彙總表
恢復正常運作（Yes）	資通安全處理小組	
召開檢討會議	資訊安全長	
異常改善及處理	資通安全處理小組	
紀錄保存	相關業務承辦人員	

5.2. 發現資訊安全事件

5.2.1. 若發現或疑似資訊安全事件時，由發現人員依事件歸屬迅速通報相關權責人員，並告知直屬單位主管。

5.2.2. 資通安全處理小組於收到通知後，研判是否為資訊安全事件。

5.2.2.1. 若判定為非資訊安全事件時，將結果回覆發現人，並協助處理及解決問題。

5.2.2.2. 若判定為資訊安全事件時，則需依資訊安全事件之影響程度通知權責主管。

5.2.3. 資訊安全事件之分類

5.2.3.1. 重大/緊急事故（服務中斷，無法於目標回復時間內恢復之事故）

5.2.3.1.1. 天然災害造成服務中斷，如：火災、地震、水災、颱風等。

5.2.3.1.2. 機房重要機電設施失效，如：不斷電系統、電力或冷氣空調失效。

5.2.3.1.3. 內部業務系統異常

A. 硬體設備故障，如主機及磁碟陣列失效。

B. 網路服務中斷，如區域網路、聯外數據線路失效。

C. 軟體異常，如資料庫、應用系統、作業系統失效。

5.2.3.1.4. 外部攻擊造成系統異常

A. 駭客入侵導致服務中斷。

B. 遭受病毒侵襲。

5.2.3.1.5. 人員操作錯誤

A. 處理人員未遵守相關作業程序。

B. 廠商維修及維護人員未依規定執行變更作業。

C. 人為破壞、疏失、洩漏機敏資訊或違反安全規定之行為，屬情節重大者。

5.2.3.1.6. 重大疾病或傳染病事件發生。

5.2.3.2. 一般安全事故（可於目標回復時間內回復之事故）

5.2.3.2.1. 設備、硬體、軟體、電力、網路失效。

5.2.3.2.2. 部分個人電腦（含終端機或查驗設備）故障或週邊設備故障。

5.2.3.2.3. 軟體失效（資料庫、應用系統、作業系統）。

5.2.3.2.4. 洩漏一般資訊或違反安全規定之行為或人為疏失，屬情節輕微者。

5.2.3.2.5. 駭客入侵惟未造成服務中斷。

5.2.3.2.6. 遭受病毒侵襲。

5.2.4. 資通安全處理小組於發生資訊安全事件時，應將事件發生之事實、可能影響之範圍、損失評估、判斷支援申請、採取之應變措施等事項，詳細記錄於「ISMS-P-009-01 資訊安全事件報告單」中。

5.3. 發出通報

5.3.1. 資訊安全事件發生時，應先研判本校資訊安全事件分類與「國家資通安全會報」資訊安全事件等級之對應。

5.3.2. 「國家資通安全會報」資訊安全事件等級共分為 4 級，如下說明。

評估類別 / 影響等級	機密性	完整性	可用性
1 級	非核心業務資料遭洩漏	非核心業務系統或資料遭竄改	非核心業務運作遭影響或短暫停頓
2 級	非屬密級或敏感之核心業務資料遭洩漏	核心業務系統或資料遭輕微竄改	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。

3 級	密級或敏感公務資料遭洩漏	核心業務系統或資料遭嚴重竄改	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。
4 級	國家機密資料遭洩漏	重要資訊基礎建設系統或資料遭竄改	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。

5.3.3. 進行資訊安全事件處理，「4」、「3」級事件須於 36 小時內復原或完成損害管制；「2」、「1」級事件須於 72 小時內復原或完成損害管制。

5.3.4. 資訊安全事件若危及人民生命或涉及民、刑事案件時，本校各單位應即時通報檢調單位協助處理。

5.3.5. 與外單位交流

各單位間應加強合作協調，實施項目如下：

5.3.5.1. 應與外部的資訊專家或顧問加強協調聯繫，相互合作，以評估單位面臨資安威脅之處理措施。

5.3.5.2. 與業務上有密切關係之機關，建立及維持適當互動管道，以利發生資安危機時，可獲得外部支援解決問題。

5.3.5.3. 對各項資訊業務委外合作廠商，應於合約規範建立資通安全及防衛網路攻擊之環境。

5.3.5.4. 記錄本校資訊安全事項之文件或資訊，於提供外界使用及經驗交流時，應予適當限制，以防敏感性資訊遭未經授權者任意取得。

5.3.6. 通報程序

當本校資訊系統發生異常狀況，應採取以下的通報程序處理。

5.3.6.1. 資通安全處理小組應視事故類型採取應變程序因應，必要時得進行系統切換作業，並完成通報作業。

5.3.6.2. 相關權責主管接獲通報後，視事故發生原因與處理狀況成立緊急處理小組進行異常事故排除，並將目前處理狀況持續向相關權責主管報告。

5.3.6.3. 通報作業

5.3.6.3.1. 資訊安全事件發現後，發現人員應以電話通知資通安全處理小組，並由資通安全處理小組權責人員填寫「ISMS-P-009-01 資訊安全事件報告單」向主管報告，並視情況逐層向資訊安全長報告。

5.3.6.3.2. 相關權責人員初步判斷事故原因，視情況尋求維護廠商或本校相關人員協助判斷，並將判斷的結果先以電話向主管報告，然後再填具至「ISMS-P-009-01 資訊安全事件報告單」中，並由主管視情況逐層向資訊安全長報告。相關權責人員需視情況通知維護廠商及本校相關人員處理修復事宜，並持續報告處理狀況。

5.3.6.3.3. 事件處置完成並確認一切回復正常運作後，相關權責人員須將處置之結果記錄於「ISMS-P-009-01 資訊安全事件報告單」中，再由主管視情況逐層向資訊安全長報告。

5.3.6.3.4. 「ISMS-P-009-01 資訊安全事件報告單」之結果內容應將資訊安全事件發生時間、發生狀況、處理結果等詳細記載。

5.3.7. 通報對象及方式

資訊安全事件通報對象、通報方式及處置期限如下表所示。

<table>
<tr><th>資訊安全
事件等級</th><th>通報對象</th><th>通報
時段</th><th>通報
方式</th><th>結案期限
(目標值)</th><th>結案
通報方式</th></tr>
<tr><td>第 1 級
(輕微)</td><td>單位主管</td><td rowspan="5">7x24
小時</td><td rowspan="5">電話
(郵件)</td><td>接獲通報後
72 小時以內</td><td rowspan="5">電話
(郵件)
資訊安全事
件報告單</td></tr>
<tr><td>第 2 級
(注意)</td><td>單位主管</td><td>接獲通報後
72 小時以內</td></tr>
<tr><td rowspan="2">第 3 級
(重大)</td><td>單位主管</td><td rowspan="2">接獲通報後
36 小時以內</td></tr>
<tr><td>資訊安全長</td></tr>
<tr><td>第 4 級</td><td>單位主管</td><td>接獲通報後</td></tr>
</table>

(嚴重)	資訊安全長			36 小時以內	

5.4. 執行各項危機處理

5.4.1. 當事件影響較低、衝擊性較小，僅涉及單位內部且受損程度輕微時（如內部小範圍電腦病毒感染），由發生事件之業務單位派員處理。

5.4.2. 處理過程中如發現造成之影響大於原先判定事件，應重新執行事件分析辨識，並依資訊安全事件通報規定重新進行通報。

5.4.3. 處理資訊安全事件時，若需其他資源，則由資訊安全長負責溝通協調作業，並適時提供資通安全處理小組必要的協助。

5.4.4. 有關是否啟動業務持續計畫，依「ISMS-P-006 業務持續管理程序書」之規定辦理。

5.4.5. 當資訊安全事件發生需對外說明時，主管須向資訊安全長詳細報告事件情況與處置方式，並由資訊安全長對外說明，視情況向上級主管機關陳報。

5.4.6.

5.4.7. 如遇資訊安全事件危及人員生命或設備遭到破壞時，情況緊急需當下處理時，由資訊安全長及時協調相關單位共同處理。

5.4.8. 危機處理程序

本校資訊安全危機處理包括事前建置安全防護機制、事中主動預警緊急應變及事後復原追蹤鑑識偵查等步驟。說明如下：

5.4.8.1. 事前建置安全防護機制

5.4.8.1.1. 建置資訊安全系統及整體防護架構，增加防禦能力，以減少事件發生。事前完備的防護機制，可增進處理事件之應變速度及減少損害程度。

5.4.8.1.2. 彙整資安文件：資訊安全相關文件應齊備，以利資訊安全事件發生時可參考使用。

5.4.8.2. 事中主動預警、緊急應變

5.4.8.2.1. 事件辨識：其目的為辨識資訊安全事件之歸屬及採取之對策為何？屬內部危安事件、外力入侵事件、天然災害或突發事件，並決定問題處理的方法與程序。

5.4.8.2.2. 事件控制：依據各類資訊安全事件危機處理之程序，進行資訊安全事件傷害控制，降低影響的程度及範圍。

5.4.8.2.3. 問題解決：資訊安全事件處理權責單位或負責人須將問題徹底解決。例如在處理電腦病毒的擴散時，採用掃毒軟體來移除主機上的病毒，將系統恢復至資訊安全事件發生前的正常運作狀態。

5.4.8.3. 事後復原追蹤鑑識偵查

5.4.8.3.1. 後續追蹤的精神在於檢討原事件是否會重複發生，並審視現有環境的漏洞，藉研析相關資料以釐清事件發生的原因與責任。

5.4.8.3.2. 受損單位依復原程序實施災後復原重建。

5.4.8.3.3. 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檢警單位申請數位鑑識（電腦、網路鑑識）。

5.4.8.3.4. 為有效追蹤，檢討事件原因，應審視現有環境的漏洞，細節記錄於「ISMS-P-009-01 資訊安全事件報告單」。

5.4.9. 判斷各類資訊安全事件並啟動相對應之緊急應變與危機處理作業程序，以進行復原工作，如下說明：

5.4.9.1. 軟、硬體故障事件（如：軟體失效、主機設備及機房重要機電設施故障），則依據「ISMS-W-004 軟硬體故障緊急應變作業標準書」之規定進行復原處理。

5.4.9.2. 網路服務中斷事件（如：連外網路、區域網路中斷），則依據「ISMS-W-005 網路連線中斷緊急應變作業標準書」之規定進行復原處理。

5.5. 評估

5.5.1. 各項資訊安全事件處理完畢後，相關會辦單位須於「ISMS-P-009-01 資訊安全事件報告單」簽名確認，並呈報主管。

5.5.2. 主管需對資訊安全事件處理結果，進行評估作業，判斷資訊安全事件所造成之影響與衝擊已獲得改善與控制，且恢復正常運作後，於「ISMS-P-009-01 資訊安全事件報告單」中簽名。

5.5.3. 主管須委派專人將「ISMS-P-009-01 資訊安全事件報告單」彙總於「ISMS-P-009-02 資訊安全事件報告彙總表」中，進行資訊安全事件列管，建立資訊安全事件學習機制，作為日後檢討與改善之依據。

5.5.4. 若無法解決及處理資訊安全事件，則持續執行各項應變計畫及危機處理作業，直至問題獲得改善與解決為止。

5.6. 召開檢討會議

若為重大資訊安全事件，於處理完畢且獲得妥善控制後，為落實預防管理及確保資訊安全事件不再重複發生，必須由資訊安全長或由主管指派專人召集相關單位召開資訊安全事件檢討會議，研析問題發生之原因。

5.7. 異常改善及處理

依據資訊安全事件檢討會議之結果，由系統負責人依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正措施，進行問題矯正的作業，以降低事件再發生的可能性。

5.8. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	資訊安全事件報告單	資網中心	至少 1 年
2	資訊安全事件報告彙總表	資網中心	至少 1 年

6. 附件

6.1. ISMS-P-009-01 資訊安全事件報告單。

6.2. ISMS-P-009-02 資訊安全事件報告彙總表。