管理系統文件

文 件 類 別	第 二 階 文 件	
文 件 編 號	IMS-P-009	
文 件 名 稱	資通安全事件管理程序書	
發 行 單 位	國立虎尾科技大學	
發 行 日 期	110 年 03 月 29 日	
版　　次	2.1	
適用單位/範圍	全校 (凡業務涉及個資蒐集、處理、利用之單位皆適用之)	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
1.1	107/08/24	增訂 5.3.3 (判定資通安全事故)
2.0	108/08/21	因應「臺灣學術網路各級學校資通安全通報應變作業程序」修訂相關作業規範與用詞。(5.3.1、5.3.2、5.3.4、5.3.7.3、5.4.7.3.1、5.4.7.3.6、5.9 情資分享辦法)
2.1	110/03/29	3.參考文件刪除「附錄 A 資通安全管理規範」，增訂「國際標準資訊安全管理系統(ISO27001：2013)」。

1. 目的

1.1 為使本校資通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 確保本校於資通安全事件發生時，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

本校與資通安全相關作業環境中之資通安全事件的管理。

3. 參考文件

3.1 臺灣學術網路各級學校資通安全通報應變作業程序。

3.2 國際標準資訊安全管理系統(ISO27001：2013)。

3.3 教育體系資通安全暨個人資料管理規範。

3.4 IMS-P-006 業務持續管理程序書。

3.5 IMS-P-008 矯正預防及持續改善管理程序書。

4. 名詞定義

4.1 資通安全事件：凡於資通作業環境中，資訊或資通系統之機密性、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（臨時員工或委外廠商派駐本校人員），發現疑似資通安全事件時，皆負有即時通報之責任。

4.3 復原目標時間（Recovery Time Objective, RTO）

資通安全事故發生後，關鍵營運流程中所有相關聯之利害關係者，所期望營運流程中斷復原之時間點。

5. 作業內容

5.1 資通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	資通安全事件報告單
發出通報	IMS 推動小組	資通安全事件報告單
執行各項危機處理	IMS 推動小組	資通安全事件報告單
評估（No）	單位主管/ 資通安全長	資通安全事件報告單 資通安全事件報告彙總表
評估（Yes）→ 恢復正常運作	IMS 推動小組	
召開檢討會議	單位主管/ 資通安全長	
異常改善及處理	IMS 推動小組	
紀錄保存	IMS 推動小組	

5.2　發現資通安全事件

5.2.1　若發現或疑似資通安全事件時，由發現人員依事件歸屬迅速通報「IMS 推動小組」，並告知直屬單位主管。

5.2.2　「IMS 推動小組」於收到通知後，研判是否為資通安全事件。

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

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

5.2.3　資通安全事件之分類

5.2.3.1　重大/緊急事件
服務中斷，無法於目標回復時間(RTO)內恢復之事件。

5.2.3.1.1　天然災害所造成的服務中斷，例如：火災、地震、水災及颱風等。

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

5.2.3.1.3　內部核心業務系統異常，無法提供正常服務。

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. 委外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　一般安全事件
可於目標回復時間(RTO)內回復之事件。

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　「IMS 推動小組」於發生資通安全事件時，應將事件發生之原因、影響等級、可能影響範圍、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「IMS-P-009-01 資通安全事件報告單」中。

5.3　發出通報

5.3.1　資通安全事件發生時，應依「臺灣學術網路各級學校資通安全通報應變作業程序」之資通安全事件等級分級。

5.3.2　資通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	非核心業務資訊遭輕微洩漏	非核心業務資訊或非核心資通系統遭輕微竄改	非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響

2 級	非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏	非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改	非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作
3 級	未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏	未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改	未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作
4 級	一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏	一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改	涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作

資安預警事件	凡屬有待受害單位進行確認之資安事件皆屬於資安預警事件，說明如下： 1. 未確定事件或待確認事件單：來自北區教育學術資通安全監控中心（N-ASOC）、南區教育學術資通安全監控中心（S-ASOC）、縣市網資通安全維運中心（MINI-SOC）使用之新型技術所產生之事件單，但正確性有待確認者。 2. 其他單位所告知教育部所屬單位所發生未確定之資安事件。

5.3.3　資通安全事件影響等級為「3 級」、「4 級」為資通安全事故，於事故處理完成後應填寫「矯正及預防措施處理單」並統一列管，以作為後續事故學習之文件，應主動提供相關設備系統日予雲嘉區網中心及臺灣學術網路通報應變小組，請求相關協助，並於一個月內將調查、處理及改善報告函送教育部，由教育部彙送主管機關。

5.3.4　進行資通安全事件處理，「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。

5.3.5　資通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。

5.3.6　與外單位交流

各單位間應加強合作協調，實施項目如下：

5.3.6.1　應與外部的資通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。

5.3.6.2　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。

5.3.6.3　對各項資通業務委外廠商，應於契約規範建立資通安全及防衛網路攻擊之環境。

5.3.6.4　記錄本校資通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。

5.3.7 通報程序

當本校資通系統發生異常狀況，應採取以下的通報程序處理。

5.3.7.1 「IMS 推動小組」應視事件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。

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

5.3.7.3 通報作業

5.3.7.3.1 資通安全事件發現後，發現人員應以電話通知「IMS 推動小組」，經確認為資安事件後須於 1 小時內，至通報應變網站通報登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。

5.3.7.3.2 權責人員填寫「ISMS-P-009-01 資通安全事件報告單」向主管報告，並視情況逐層向資通安全長報告。

5.3.7.3.3 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於確認資安事件條件成立後 1 小時內，與所屬區、縣（市）網路中心及通報應變小組聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。

5.3.7.3.4 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。

5.3.7.3.5 事件處置完成並確認一切回復正常運作後，相關權責人員須至通報應變網站通報結案，並登錄資安事件處理過程及完成時間，並將處置之結果記錄於「ISMS-P-009-01 資通安全事件報告單」中，再由主管視情況逐層向資通安全長報告。

5.3.7.3.6 「4」、「3」級資安事件完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內將

調查、處理及改善報告函送上級機關或監督機關。

5.3.7.3.7　確認為資安事件後，須於 1 小時內，至臺灣學術網路危機處理中心之通報應變網站登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。

5.3.7.3.8　如因網路或電力中斷等事由，致使無法上網填報資安事件，須於確認資安事件條件成立後 1 小時內，與所屬區、縣（市）網路中心及通報應變小組聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。

5.3.7.3.9　如因網路問題無法通報，可填寫「臺灣學術網路各級學校資通安全事件通報單」以傳真或電子郵件方式送至「臺灣學術網路危機處理中心」進行通報。

5.3.7.3.10　完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理過程及完成時間。

5.3.8　通報對象及方式

資通安全事件通報對象、通報方式及處置期限如下表所示。

<table>
<tr><th>資通安全事件等級</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="6">7x24小時</td><td rowspan="6">電話(郵件)</td><td>接獲通報後72 小時以內</td><td rowspan="6">電話(郵件)資通安全事件報告單</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>資通安全長</td></tr>
<tr><td rowspan="2">第 4 級(嚴重)</td><td>單位主管</td><td rowspan="2">接獲通報後36 小時以內</td></tr>
<tr><td>資通安全長</td></tr>
</table>

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，並依資通安全事件通報規定重新進行通報。

5.4.3 處理資通安全事件時，若需其他資源，則由資通安全長負責溝通協調作業，並適時提供「IMS 推動小組」必要的協助。

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

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

5.4.6 如遇資通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，由資通安全長及時協調相關單位共同處理。

5.4.7 危機處理程序

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

5.4.7.1 事前建置安全防護機制

5.4.7.1.1 建置資通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。

5.4.7.1.2 彙整資安文件：資通安全相關文件應齊備，以利資通安全事件發生時可參考使用。

5.4.7.1.3 核心資通系統應依「資通安全責任等級分級辦法」規定進行盤點作業，判定資通系統安全防護等級，並據以落實資安防護基準。

5.4.7.1.4 資通安全整體防護環境與內部資料存取控制應依「IMS-P-013 帳號密碼及存取控制管理程序書」與「IMS-P-011 實體與環境安全管理程序書」之規定辦理。

5.4.7.1.5 資通安全防護、入侵偵測、安全檢測、弱點掃描及網路監控等作業應依「IMS-P-012 網路安全管理程序書」之規定辦理。

5.4.7.1.6　系統與資料備份應依「IMS-P-015 資訊備份管理程序書」之規定辦理。

5.4.7.1.7　資通安全稽核應依「IMS-P-007 資安及個資內部稽核作業管理程序書」之規定辦理。

5.4.7.1.8　人員安全管理與資安認知教育訓練應依「IMS-P-010 人力資源安全與訓練管理程序書」之規定辦理。

5.4.7.1.9　資安紀錄與系統日誌之保留應依「IMS-P-001 文件與紀錄管理程序書」之規定辦理。

5.4.7.1.10　資通委外服務應依「IMS-P-018 資通業務委外作業管理程序書」之規定辦理。

5.4.7.2　事中主動預警、緊急應變

5.4.7.2.1　事件辨識：其目的為辨識資通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。

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

5.4.7.2.3　問題解決：資通安全事件處理權責單位或負責人須將問題徹底解決，使系統恢復至資通安全事件發生前的正常運作狀態。

5.4.7.2.4　查詢臺灣學術網路危機處理中心網站、系統弱點(病毒)資料庫或聯絡技術支援單位(廠商)等方式，以尋求解決方案；如無法解決，應儘速向所屬區、縣（市）網路中心及通報應變小組反應，請求提供相關技術支援。

5.4.7.2.5　評估資安事件對業務運作造成之衝擊，並進行損害管制。若未納入本校防護範圍之資通系統發生資安事件，為防止損害擴大影響他人或正常使用者之權益，依據「臺灣學術網路管理規範」，得先行中斷發生資安事件之系統網路連線，待該系統完成通報應變改善作為後，始得恢復其連線。

5.4.7.2.6　視資安事件損壞程度，遵循「IMS-P-006 業務持續管理程序書」之規定，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。

5.4.7.3　事後復原追蹤鑑識偵查

5.4.7.3.1　全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫，細節記錄於「ISMS-P-009-01 資通安全事件報告單」。

5.4.7.3.2　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。

5.4.7.3.3　受損單位依復原程序實施災後復原重建。

5.4.7.3.4　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）。

5.4.7.3.5　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「IMS-P-009-01 資通安全事件報告單」。

5.4.7.3.6　資通安全事件調查、處理及改善報告，應包括下列事項：

A. 事件發生或知悉其發生、完成損害控制或復原作業之時間。

B. 事件影響之範圍及損害評估。

C. 損害控制及復原作業之歷程。

D. 事件調查及處理作業之歷程。

E. 事件根因分析。

F. 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

G. 前款措施之預定完成時程及成效追蹤機制。

5.5　評估

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

5.5.2 主管需對資通安全事件處理結果，進行評估作業，判斷資通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「IMS-P-009-01 資通安全事件報告單」中簽名。

5.5.3 「IMS 推動小組」須將「IMS-P-009-01 資通安全事件報告單」彙總於「IMS-P-009-02 資通安全事件報告彙總表」中，進行資通安全事件列管，建立資通安全事件學習機制，作為日後檢討與改善之依據。

5.5.4 若無法解決及處理資通安全事件，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。

5.5.5 「2」、「1」級資安事件通報應變完成後，應至通報應變網站列印單件，每月彙整送呈單位主管。

5.6 召開檢討會議

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

5.7 異常改善及後續處理

5.7.1 依據資通安全事件檢討會議之結果，由系統負責人依據「IMS-P-008 矯正預防及持續改善管理程序」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。

5.7.2 資通安全事件完成矯正及預防措施後，需由業務承辦人員針對發生事件之根因進行風險再評估作業，確認此風險已排除並受到適當之控制。

5.8 資安演練作業

5.8.1 每年遵循教育部「資通安全通報演練」計畫，針對演練模擬事件，研擬應變處理作為，並於「各級學校資安通報演練平台」回復應變處理作為。

5.8.2 每年遵循教育部「防範惡意電子郵件社交工程演練」計畫，針對演練模擬事件，回報受測人員之公務電子郵件名單參與演練。

5.9 情資分享辦法

當有下列各項情況，應予以情資分享：

5.9.1 資通系統之惡意偵察或情蒐活動。

5.9.2 資通系統之安全漏洞。

5.9.3 使資通系統安全控制措施無效或利用安全漏洞之方法。

5.9.4 與惡意程式相關之資訊。

5.9.5 資通安全事件造成之實際損害或可能產生之負面影響。

5.9.6 用以偵測、預防或因應前五款情形，或降低其損害之相關措施。

5.9.7 其他與資通安全事件相關之技術性資訊。

5.10 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	資通安全事件報告單	電子計算機中心	至少 3 年
2	資通安全事件報告彙總表	電子計算機中心	至少 3 年

6. 附件

6.1 IMS-P-009-01 資通安全事件報告單。

6.2 IMS-P-009-02 資通安全事件報告彙總表。