國立臺南藝術大學
安全事件管理程序書

機密等級：限閱

文件編號：IS-B-012

版　　次：3.2

發行日期：111.08.02

安全事件管理程序書					
文件編號	IS-B-012	機密等級	限閱	版本	3.2

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	100/03/14		李立明	初版
1.1	100/04/07	7	方惠卿	刪除5.3.3.3
1.2	100/04/15	5~14	方惠卿	1.修訂資安事件通報應變程序。 2.新增資安事件通報與應變流程附件。
1.3	103/02/26	9、15	陳智堯	增訂異常事件紀錄表流程
1.4	104/03/19	6、7	方惠卿	資安事件項目等級區分內容修訂
1.5	104/04/22	5、10	李立明	3.增訂資安事件區分。 4.修訂異常事件紀錄表填寫時機。
1.6	108/10/08	目錄~14、1~6、10、11	王靜怡	因應資通安全法及子法施行修訂 1.修改目錄及分頁項目樣式，並將資訊安全事件修改為資安事件。 2.修改資安事件名詞定義。 3.將資安事件的「一般性異常事件」的「一般性」刪除，並將資通安全事件影響等級修改為四級。 4.刪除主管機關（教育部）並修改通報機關（本校）內容。 5.修改資安事件項目等級區分四個級別內容。 6.新增資安事件通報應變流程(五)。 7.修改相關文件為資通安全事件通報及應變辦法。

3.0	109/9/25	4~14	詹怡珊	依「教育體系資通安全暨個人資料管理規範」、ISO 27001：2013版修訂、修改 貳、參考依據 參、適用範圍 肆、權責 伍、名詞定義 陸、作業說明 柒、輸出表單／紀錄
3.1	110/11/19	7、10~14		依「臺灣學術網路各級學校資通安全通報應變作業程序」修改 (二) 資訊安全事件項目等級區分 1. 通報及應變流程 3. 事後復原追蹤鑑識偵查
3.2	111/08/02	4、5、10、11、12	詹怡珊	1. 參考依據新增三、資通安全事件通報及應變辦法 2. 修訂餘逾文字 3. 修訂秘書裁定內容 4. 修訂資訊系統名稱 5. 修訂資安處理分組內容

目錄

壹、目的

確保國立臺南藝術大學（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。

貳、參考依據

一、 IS-A-002-臺南藝術大學資安政策

二、 臺灣學術網路各級學校資通安全通報應變作業程序

三、 資通安全事件通報及應變辦法

四、 教育部資通安全處理小組作業說明

五、 教育體系資通安全暨個人資料管理規範：2019年版

六、 ISO/IEC 27001：2013

參、適用範圍

本程序書適用於本校資訊安全事件管理。

肆、權責

一、 ISMS推動小組

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。

二、 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。

三、 權責單位

(一) 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。

(二) 資訊安全事件內部、弱點通報。

(三) 確定事件影響範圍，並評估損失。

四、 執行秘書

(一) 督導資訊安全事件通報、處理及分析作業。

五、 資安處理組

(一) 研擬本校「資訊安全事件通報與應變作業流程」。

(二) 協助資訊安全事件之通報、處理及分析作業，協助評估事件影響範圍及損失。

(三) 處理資訊機房實體環境、網路、維運系統之資安問題。

(四) 研判、分派、處理不明原因或各單位難以辨別之資安事件。

(五) 管制資安事件處理進度。

六、 支援單位

(一) 內部單位：協助處理相關法律、人事懲處及採購等問題。

(二) 委外廠商：協助處理資訊安全事件。

伍、名詞定義

一、 資訊安全事件

任何違反常軌的異常行為，其可能造成資訊、系統、網路、營運中斷的安全威脅從設備故障、人員差錯、人爲因素或自然災害所造成的災害或損失均稱為事件，事件可為單一事件到各種複雜的事件。

二、 資訊安全事件

單一或一連串已危害組織營運或或發生立即性威脅資訊安全措施的資訊安全事件。

陸、作業說明

一、 資訊安全事件的定義及等級

(一) 資訊安全事件區分

1. 一般性異常事件：電腦設備、應用系統、網路或資料庫發生異常或人為操作不當，可迅速完成處理、故障排除或可立即由其他備援、餘逾設備取代，未造成本校作業影響。
2. 資訊安全事件：電腦設備、應用系統、網路或資料庫發生異常或人為操作不當，無法立即完成處理，或無法透由其他備援、餘裕設備取代，造成本校部份或全部業務、系統、網路停頓，或造成資料損毀、遭違法竄改、外洩、竊取，已造成本校資訊資產之機密性、完整性、可用性危害的突發事件，或遭駭客、病毒攻擊已大範圍擴散，甚而成為跳板轉而攻擊其他機關之事件。

(二) 資訊安全事件項目等級區分

1. 依據資通安全事件通報及應變辦法規定，影響等級由輕至重分「零」「一」、「二」、「三」、「四」五個級別，評定資訊安全事件影響等級時，將以該事件造成之三面向（機密性、完整性及可用性）衝擊性，綜評該事件影響等級，以三個層面向最高者為其影響等級，資訊安全事件一到四級評定方式如下表：

等級	機密性	完整性	可用性
四	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。
三	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。
二	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	非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，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

		心資通系統遭輕微竄改。	
一	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.「零」級事件（資安預警）

資安事件造成之「機密性」、「完整性」及「可用性」符合下列任一情形者，凡屬於下列工單皆屬於零級事件：

(1) 未確定事件或待確認工單:來自不同計畫所使用新型技術（A-SOC，miniSOC,…）所產生之工單，但其正確性有待確認。

(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。

(3) 教育部及區、縣網路中心檢舉信箱通告之資安事件。

(4) 上述皆屬於有待受駭（害）單位進行確認之資安事件。

3. 零級事件的設立目的

(1) 提供資安預警的功能:未必每個單位會遭受到零級攻擊事件，但可提請各單位加強檢查所負責之伺服器或設備是否有遭受攻擊的可能性。

(2) 協助不同計畫所使用新型技術（A-SOC，miniSOC,…）並加強其正確性。

(3) 確認與處理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。

(4) 確認與處理教育部及區、縣網路中心檢舉信箱通告之資安事件。

(三) 資通安全事件通報處理時限

類別	通報應變作業綱要規定
評定標準	機密性、完整性、可用性
影響等級	（輕←→重）
	零、一、二、三、四
主管機關審核時間	三、四級：二小時
	零、一、二級：八小時

通報機關 結案時間	三、四級：36 小時
	零、一、二級：72 小時

1. 主管機關（教育部）

除因網路或電力中斷等事由，致無法依上級或監督機關及行政院所指定或認可之方式通報外，應於知悉資通安全事件後一小時內上級或監督機關及 行政院所指定或認可之方式，進行事件通報。

(1) 通報事件為「三」、「四」級事件，應由主管機關資通安全長進行督導。

(2)「三」、「四」級事件，須於通報後二小時內完成事件審核。

(3)「一」、「二」級事件，須於通報後八小時內完成事件審核。

2. 通報機關（本校）

發現資安事件後，須於一小時內通報登入通報平台完成通報此事件。

3.「四」、「三」級事件，須於36小時內復原或完成損害管制。

4.「一」、「二」級事件，須於72小時內復原或完成損害管制。

二、 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) 事件判斷原則：

1. 由各單位之網路負責人或本處網路負責人判斷該事件會嚴重影響網路之運作

2. 該事件影響本校校譽或形象

3. 重要系統發生資安事件

4. 由本校安全設備或軟體得知該系統進行大量攻擊

5. 系所單位之網頁遭置換或破壞

6. 經告知或自行得知該設備在進行攻擊行為

7. 遭私自建立帳號或檔案共享

8. 已清除病毒卻又感染同樣病毒

9. 不明原因之網路流量暴增

10. 其他已確定之中毒或入侵狀況

(三) 處理程序

1. 本校各單位之資訊安全事件可由該單位之資安負責人先行處理，無法解決時由資訊處資安處理組處理。

2. 處理時以該系統負責人在場為原則。

3. 處理後需告知該系統負責人或網管負責人處理過程及防範之道，並監控是否還有同樣情況或異常狀況，以避免同樣問題再度發生。

4. 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外，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。

5. 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：

(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。

(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。

(四) 證據保存

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依據。

三、 資安事件通報應變流程

依資訊安全事件通報與應變作業流程辦理，作業說明如：

(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，並副本告知直屬主管。

(二) 通報方式：電話、Email、書面。

(三) 權責單位於收到通知後，研判是否為資訊安全事件，如僅為一般性異常事件未造成本校作業影響，依相關報修程序辦理，如已構成資訊安全事件或接獲教育部通報平台、教育部區網中心、其他單位資訊安全事件通報，由資安處理組填寫「異常事件紀錄表」。

1. 判定為資訊安全事件時，由處理單位初估事件處理時間、事件等級、評估是否須通報教育部，並陳報執行秘書。

2. 經執行秘書裁示通報教育部，由資安處理組登入教育機構資安通報平台（https://info.cert.tanet.edu.tw），執行通報作業。

3. 經執行秘書裁示不通報教育部，由資安管理組管制結案。

(四) 教育機構資通安全通報應變流程：

1. 通報及應變流程

(1) 通報係由資安處理組依「異常事件紀錄表」核定通報之事件向教育部通報。不管是哪一級資安事件，當發現事件時須於1小時內登入通報平台完成通報此事件。三、四級因事態嚴重，因此尚須電話通知上層管理，落實緊急通報。

(2) 發現資安事件時，須於1小時內登入通報平台完成通報此資安事件。

A. 事件等級:因係一、二級通報，故無須電話告知區網中心人員。

B. 是否需支援:若需支援，則主動電話聯繫區網中心人員請求協助。

(3)「4」、「3」級資安事件須於 36 小時內完成損害控制或復原;「2」、「1」級資安事件須於 72 小時內完成損害控制或復原。

(4) 資安處理組完成通報處理作業，並於應變處理完成後，於資安通報平台填寫應變處理情形，辦理結案。

(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;「4」、「3」級資安事件需於事件發生後 36 小時內，通報送陳單位資通安全長。

(6) 評估資安事件對業務運作造成之衝擊，並進行損害管制。若未納入各單

位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」，各單位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。

(7) 如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予所屬區、縣(市)網路中心及通報應變小組，俾提供相關協助。

(8) 「4」、「3」級資安事件依本項規定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本(教育)部，由本(教育)部彙送主管機關。

(9) 各單位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。

四、 決策處理

(一) 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執行秘書。

(二) 處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向執行秘書報告，重新執行事件分析辨識。

(三) 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。

五、 危機處理程序

(一) 本處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ISMS推動小組會提出建議方案。

(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。

(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單位或檢警單位申請數位鑑識（電腦、網路鑑識）。

(4) 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後，即進行安全備份及資料復原等相關事宜。

(5) 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析與檢討改善方案、防止同類事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。

(6) 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。

六、 資訊安全弱點通報與處理

(一) 通報人員如發現任何系統或服務中所觀察到或可疑之資訊安全弱點，應立即向資安處理組或權責管理單位通報。

(二) 資安處理組或權責管理單位應協助判斷系統或設備之資訊安全弱點及解決方式，通知相關人員進行修補，並研判是否已構成資訊安全事件，如判定為資訊安全事件依前述規定辦理。

(三) 未經網路資訊組同意不得於本公校網路使用弱點偵測或任何利用弱點破

解工具。

七、 資訊安全事件中學習

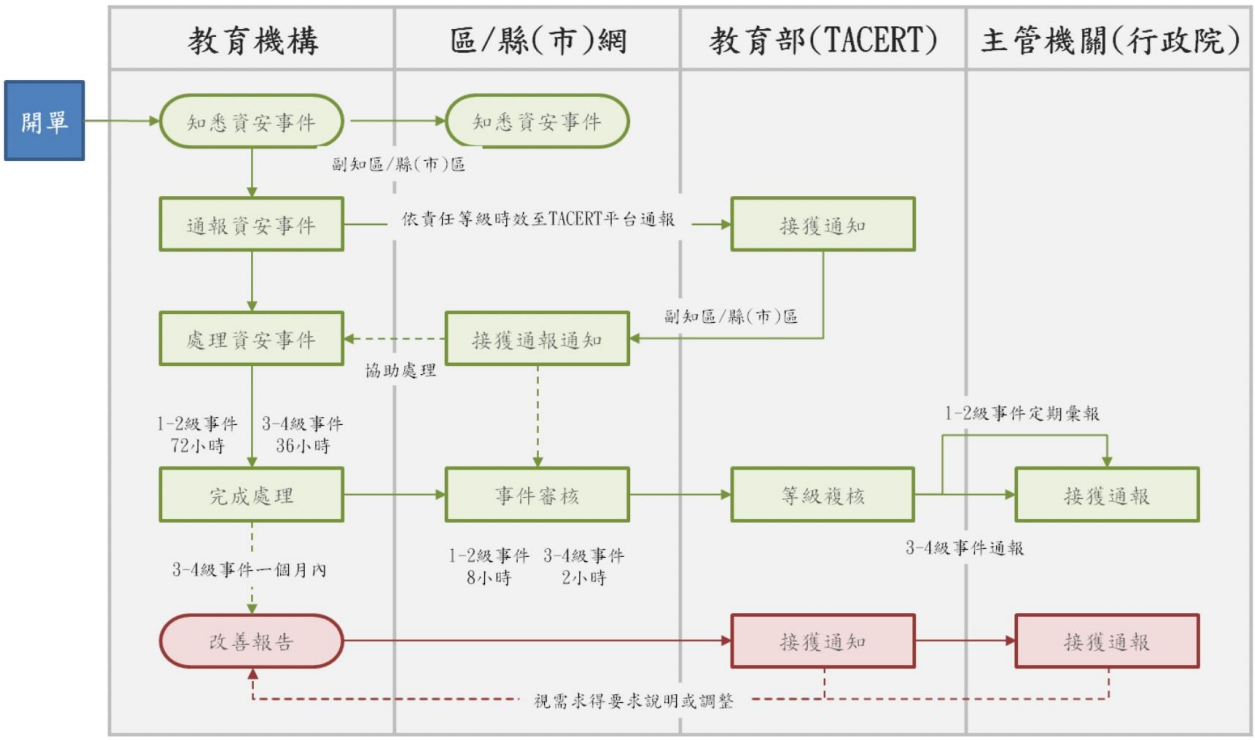
(一) 屬三級(含)以上資訊安全事件之處理結果相關資料文件，資安處理組收整後交文件管制組保存，並將事件發生原因、過程、處理方式、改善及注意事項等，做為內部資安宣導及事件預防之參考資訊，宣導內容應將個人隱私及業務機密予以遮蔽。

(二) 相關資訊安全事件或事故應回饋至風險評鑑結果。

柒、輸出表單／紀錄

一、 IS-D-055異常事件紀錄表

附件一、通報應變處理流程



附件二、資訊安全事件通報與應變作業流程圖