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	資通安全事件通報及應變管理程序書	
發 行 單 位	文 件 管 制 小 組	
發 行 日 期	108 年 04 月 15 日	
版　　次	2.2	
訂修廢單位	審　　查	核　　准
資 通 安 全 處 理 小 組		

（文件訂修廢申請紀錄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
2.0	104/04/30	2015 改版發行。
2.1	107/03/09	修改本文件資訊安全事件報告單、資訊安全事件報告彙總表保存地點資訊科技中心單位名稱為圖書資訊處。
2.2	108/04/15	因應資通安全管理法及資通安全事件通報及應變辦法修訂程序

1. 目的

1.1 本校為遵照資通安全管理法第 14 條及本校資安全維護計畫之規定，建立本校資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資訊安全事件管理程序書，其中包含資通安全事件通報及應變管理程序。

1.2 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。

1.3 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

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

3. 參考文件

3.1 資通安全管理法。

3.2 資通安全事件通報及應變辦法。

3.3 ISMS-P-006 業務持續管理程序書。

3.4 ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

4.1 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

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），發現疑似資訊安全事件時，皆負有即時通報之責任。

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

資通安全事件發生後，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. 責任權限

5.1 本校所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

5.2 本校應於資通安全事件發生前，確保同仁及權責人員熟悉資通安全事件之通報及完成應變作業程序。

5.3 本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本校進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

5.4 本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

6. 作業內容

6.1 資通安全事件通報及應變處理流程圖

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
執行各項應變處理	資通安全處理小組	資訊安全事件報告單
評估（No）	單位主管/ 管理代表	資訊安全事件報告單 資訊安全事件報告彙總表
Yes		
恢復正常運作	資通安全處理小組	
召開檢討會議	單位主管/ 管理代表	
異常改善及處理	資通安全處理小組	
紀錄保存	資通安全處理小組	

6.2　發現資通安全事件

6.2.1　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「資通安全處理小組」，並告知直屬單位主管。

6.2.2　「資通安全處理小組」於收到通知後，研判是否為資通安全事件。

6.2.2.1　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。

6.2.2.2　若判定為資通安全事件時，則應執行通報及應變事務。

6.2.2.3　本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

6.2.2.4　事件通報窗口及緊急處理小組

6.2.2.4.1　本校之資通安全事件通報窗口及聯繫專線為：

6.2.2.4.2　本校應以適當方式使相關人員明確知悉本校之通報窗口及聯絡方式。

6.2.2.4.3　本校所屬人員發現資通安全事件後，應立即向所屬單位主管及本校之通報窗口通報。

6.2.2.4.4　本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

6.2.2.4.5　負責事件處理之單位（該事件發生之單位）權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

6.2.2.4.6　事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬機關或受託

廠商所通報之資通安全事件時，亦同。

6.2.2.4.7 「緊急處理小組」成員由資通安全管理代表指派機關之資通安全相關技術人員擔任，或亦得聘任外部專家擔任之。

6.2.2.4.8 各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

6.2.3 「資通安全處理小組」於發生資通安全事件時，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 資通安全事件報告單」中。

6.3 發出通報

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

6.3.2 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。	非核心業務或非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。
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。	非核心業務或非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。

6.3.3　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。

6.3.4　與外單位交流

各單位間應加強合作協調，實施項目如下：

6.3.4.1　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。

6.3.4.2　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。

6.3.4.3　對各項資訊業務委外廠商，應於契約規範建立資訊安全及防衛網路攻擊之環境。

6.3.4.4　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。

6.3.5　通報程序

當本校發生資通安全事件，應採取以下的通報程序處理。

6.3.5.1　「資通安全處理小組」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。

6.3.5.2　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：該小組由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

6.3.5.3　本校之權責人員或緊急處理小組應於知悉資通安全事件後，依據以下事項，並依「資通安全事件通報及應變辦法」規定，完成資通安全事件等級判斷：

6.3.5.3.1　事件涉及核心業務或關鍵基礎設施業務之資訊與否。

6.3.5.3.2　事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。

6.3.5.3.3　事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

6.3.5.3.4　機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

6.3.5.3.5　事件其他足以影響資通安全事件等級之因素。

6.3.5.4　除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本校因應之能力進行評估。

6.3.5.5　本校權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全長核准。

6.3.5.6　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。

6.3.5.7 本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於知悉資通安全事件後一小時內以電話或其他適當方式，將該次資安事件應通報之內容及無法通報依規定方式通報之事由，分別告知所屬之上級或監督機關及行政院，並於事由解除後，依原方式補行通報。

6.3.5.8 資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。

6.3.5.9 本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向本校之權責人員或窗口，以指定之方式進行通報。

6.3.5.10 本校執行通報應變作業時，得視情形向本府資訊科技局提出技術支援或其他協助之需求。

6.4 執行應變程序

6.4.1 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。

6.4.2 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。

6.4.3 處理資通安全事件時，若需其他資源，則由管理代表負責溝通協調作業，並適時提供「緊急處理小組」必要的協助。

6.4.4 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。

6.4.5 當資通安全事件發生需對外說明時，主管須向管理代表詳細報告事件情況與處置方式，並由管理代表或資通安全長對外說明，視情況向上級主管機關陳報。

6.4.6 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，由管理代表及時協調相關單位共同處理。

6.4.7　應變處理程序

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

6.4.7.1　事前建置安全防護機制

6.4.7.1.1　本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

6.4.7.1.2　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。

6.4.7.1.3　彙整資安文件：資訊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。

6.4.7.2　事中主動預警、緊急應變

6.4.7.2.1　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。

6.4.7.2.2　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。

6.4.7.2.3　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。

6.4.7.3　損害控制機制

6.4.7.3.1　負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄。

A. 資安事件之衝擊及損害控制作業。

B. 資安事件所造成損害之復原作業。

C. 資安事件相關鑑識及其他調查作業。

D. 資安事件之調查與處理及改善報告之方式。

E. 資安事件後續發展及與其他事件關聯性之監控。

F. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本校事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。

G. 其他資通安全事件應變之相關事項。

6.4.7.3.2 第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄。

6.4.7.3.3 第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

6.4.7.3.4 本校完成通報及應變程序之辦理後，應依所隸屬之上級機關或行政院所指定或認可之方式進行結案登錄。

6.4.7.3.5 本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

6.4.8 事後復原追蹤、鑑識、調查及改善機制

6.4.8.1 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。

6.4.8.1.1 受損單位依復原程序實施災後復原重建。

6.4.8.1.2 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）。

6.4.8.1.3　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 資通安全事件通報單」。

6.4.8.1.4　應於事件發生後一個月內完成資通安全事件調查、處理及改善報告，內容應包括以下項目：

A. 事件發生、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. 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。

F. 前款措施之預定完成時程及成效追蹤機制。

6.4.8.1.5　本校應向所隸屬之上級機關及行政院提出前項之報告，以供監督與檢討。

6.4.8.1.6　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 資通安全事件通報單」。

6.5　評估

6.5.1　各項資通安全事件處理過程需會辦相關單位，並由相關權責人員於「ISMS-P-009-01 資通安全事件通報單」簽名確認，並呈報主管。

6.5.2　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「ISMS-P-009-01 資通安全事件通報單」中簽名。

6.5.3　「資通安全處理小組」須將「ISMS-P-009-01 資通安全事件通報單」彙總於「ISMS-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。

6.5.4　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。

6.6　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，必須由管理代表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。

6.7　異常改善及後續處理

6.7.1　依據資通安全事件檢討會議之結果，由系統負責人依據「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。

6.7.2　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。

6.8　資通安全事件通報單紀錄留存及管理程序之調整

6.8.1　本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資通安全事件通報單」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全長簽核。

6.8.2　本校於完成資通安全事件之通報及應變程序後，應依據「資通安全事件通報單」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

6.9　演練作業

6.9.1　本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

6.9.1.1　網路攻防。

6.9.1.2　情境演練。

6.9.1.3　其他資安演練。

6.10　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	資通安全事件通報單	資通安全處理小組	至少 3 年
2	資通安全事件報告彙總表	資通安全處理小組	至少 3 年

7. 附件

7.1 ISMS-P-009-01 資通安全事件通報單。

7.2 ISMS-P-009-02 資通安全事件報告彙總表。

開南大學
KAINAN University

資通安全事件通報單

事件通報單位聯絡資料			
通報人		單位名稱	
電話		電子郵件	

事件通報事項			
事件發生時間	___年___月___日___時___分	填報日期	___年___月___日___時___分
事件樣態	□資通安全事件 □個人資料事件 □重大緊急事件 □其他事件_____	管制編號	
事件說明			

設備資料 (發生事件之資訊系統的詳細資訊)				
	IP 位址		Web 位址	
	設備廠牌、機型		作業系統/版本	
	已裝置之安全機制			

資通安全事件影響等級 (以 C, I, A 最高級別為事件等級)		
	機密性衝擊 (單選)	□國家機密資料遭洩漏(4 級) □密級或敏感公務資料遭洩漏(3 級) □核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2 級) □非核心業務一般資料遭洩漏(1 級) □無資料遭洩漏(無需通報)
	完整性衝擊 (單選)	□關鍵資訊基礎設施系統或資料遭嚴重竄改(4 級) □核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3 級) □非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改(2 級) □非核心業務系統或資料遭竄改(1 級) □無系統或資料遭竄改(無需通報)
	可用性衝擊 (單選)	□關鍵資訊基礎設施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) □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；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(3 級) □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；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(2 級) □非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(1 級) □無系統或設備運作受影響(無需通報)

資通安全事件等級判定	□0 級 □1 級 □2 級□3 級 □4 級 (3 級及 4 級須呈核至管理代表以上管理階層)	□通報國家資通安全應變中心 (111.7.4 外稽建議改為教育部通報平台)
破壞程度	□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染 □個資被竊取、竄改、毀損、滅失或洩漏 □其他_____	
事件影響範圍及損失評估		

事件之應變與處置	
損害控制及復原作業之歷程	
系統服務終止紀錄(必填)	□系統維持運作，無須終止服務。 □系統需終止服務(起迄時間：　年　月　日　時　分～　年　月　日　時　分)，總停機時間：　日　時　分。
期望支援項目	
事件調查及處理作業之歷程	□另填寫「矯正及預防處理單」將此問題列管並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(預防措施)，及預定完成時程和成效追蹤機制納入管制。

完成損害控制或復原作業之時間	_____年_____月_____日_____時_____分

承辦單位	會辦單位	管理代表	資通安全長

開　南　大　學
K A I N A N University

資通安全事件報告彙總表

編號	發生日期	發生單位	資通安全事件說明	影響等級	事件分類	破壞程度	解決日期
				□1 級 □2 級 □3 級 □4 級	□資通安全事件 □個人資料事件 □重大緊急事件 □其他事件____________	□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染 □個資被竊取、竄改、毀損、滅失或洩漏 □其他_________________	
				□1 級 □2 級 □3 級 □4 級	□資通安全事件 □個人資料事件 □重大緊急事件 □其他事件____________	□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染 □個資被竊取、竄改、毀損、滅失或洩漏 □其他_________________	
				□1 級 □2 級 □3 級 □4 級	□資通安全事件 □個人資料事件 □重大緊急事件 □其他事件____________	□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染 □個資被竊取、竄改、毀損、滅失或洩漏 □其他_________________	
				□1 級 □2 級 □3 級 □4 級	□資通安全事件 □個人資料事件 □重大緊急事件 □其他事件____________	□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染 □個資被竊取、竄改、毀損、滅失或洩漏 □其他_________________	