大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-程序-23	文件名稱	資訊安全事件通報及危機處理管理程序書
使用部門	圖書資訊館	機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	8	初版	99/05/24

訂修廢者	單位主管	資訊安全長

※管制文件不得擅自塗改及做記號並禁止影印。

1.目的

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 資訊-程序-16 業務持續管理程序書。

3.2 資訊-程序-22 資訊設備維護與管理程序書

3.3 資訊-標準-04 網路連線中斷緊急應變作業標準書

3.4 資訊-標準-05 外力入侵事件緊急應變作業標準書

3.5 資訊-標準-06 天然災害事件緊急應變作業標準書

3.6 資訊-程序-08 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 資訊安全事件分類

4.2.1 內部資安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎或電腦病毒感染等危安事件。

4.2.2 外力入侵事件：電腦病毒感染事件、駭客攻擊（或非法入侵）事件。

4.2.3 天然災害或突發事件

4.2.3.1 天然災害：颱風、水災、地震等。

4.2.3.2 突發事件：火災、爆炸、核子事故、建築災害及資訊網路系統骨幹（主幹寬頻）中斷事件等。

4.3 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

流程	權責	相關文件
發現資安事件	發現人員	資訊安全事件報告單
發出通報	圖書資訊館	
執行各項危機處理	圖書資訊館	各項緊急應變作業標準書
評估（No）	權責主管	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）	圖書資訊館	
召開檢討會議	資訊安全長	
異常改善及處理	圖書資訊館	
紀錄保存	圖書資訊館	

5.2 發生資訊安全事件

5.2.1 疑似資訊安全事件發生時,由發現人員依事件歸屬通報圖書資訊館並告知直屬單位主管。

5.2.2 圖書資訊館於收到通知後，研判是否資訊安全事件。若：

5.2.2.1 判定為非資安事件時，將結果回覆發現人，並協助處理及解決問題。

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

5.2.3 資訊安全事件等級區分為 4 級：

評估類別 / 影響等級		機密性	完整性	可用性
輕微 ↓ 嚴重	1 級	屬「普通」等級資料遭洩漏	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	屬「內部使用」等級業務資料遭洩漏	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，於可容忍中段時間內回復正常運作
	3 級	屬「密」等級資料遭洩漏	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，無法於可容忍中段時間內回復正常運作
	4 級	屬「密」等級資料遭洩漏	本校重要資訊基礎建設系統或資料遭竄改	本校重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中段時間內回復正常運作

5.2.4 圖書資訊館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「資訊-程序-23-01 資訊安全事件報告單」中。

5.3 發出通報

5.3.1 圖書資訊館於收到通知後，若判定為資訊安全事件時，依下列之規定進行資訊安全事件之通報。

資訊安全事件通報規定	
資安事件影響等級	通報等級
1 級	單位主管
2 級	圖書資訊館館長
3 級	資訊安全長(副校長)
4 級	校長/上級單位

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、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通知圖書資訊館派員處理。

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，並依資安事件通報規定重新進行通報。

5.4.3 處理資安事件時，若需其他資源，則由資訊安全長負責溝通協調作業，並適時提供緊急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「資訊-程序-16 業務持續管理程序書」之規定辦理。

5.4.5 有關本校資訊設備發生異常則依「資訊-程序-22 資訊設備維護與管理程序書」進行處理。

5.4.6 當資安事件發生需對外說明時,由圖書資訊館館長協助公關部門對外說明情況與處置方式，並向上級主管機關陳報。

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 參考「行政院及所屬各機關資訊安全管理要點、管理規範」規劃建置資安系統及網路安全整體防護環境。

5.4.8.1.3 彙整資安文件：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。

5.4.8.2.3 問題解決：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 資安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，由圖書資訊館將細節紀錄於「資訊-程序-23-01 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 網路連線中斷事件，則依據「資訊-標準-04 網路連線中斷緊急應變作業標準書」之規定進行復原處理。

5.4.9.2 外力入侵事件，則依據「資訊-標準-05 外力入侵事件緊急應變作業標準書」之規定進行復原處理。

5.4.9.3 天然災害或突發事件，則依據「資訊-標準-06 天然災害事件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，圖書資訊館及相關會辦單位須於「資訊-程序-23-01 資訊安全事件報告單」簽名確認，並呈報權責主管。

5.5.2 權責主管需對資安事件處理結果，進行評估作業，判斷資安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「資訊-程序-23-01 資訊安全事件報告單」中簽名。

5.5.3 圖書資訊館館長須委派專人將「資訊-程序-23-01 資訊安全事件報告單」彙總於「資訊-程序-23-02 資訊安全事件報告彙總表」中，進行資安事件列管，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安事件,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(資安等級 3 級以上),於處理完畢且獲得妥善控制後，為落實預防管理確保資安事件不再重複發生，必須由資訊安全長或由資訊安全長指派專人召集相關單位召開資安事件檢討會議，研析問題發生之原因。

5.7 異常改善及處理

依據資安事件檢討會議之結果,由圖書資訊館系統負責人依據「資訊-程序-08 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.附件

6.1 資訊-程序-23-01 資訊安全事件報告單

6.2 資訊-程序-23-02 資訊安全事件報告彙總表。