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-15	文件名稱	資訊安全事件管理程序書	
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	4	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

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，特制訂本程序書。

2.適用範圍

凡本校資訊安全事件之管理，均適用本程序書。

3.參考文件

3.1 資訊-程序-23 資訊安全事件通報及危機處理程序書。

4.名詞定義

4.1 資訊安全事件：凡於作業環境中，資訊之機密性、完整性、可用性遭受破壞之事件。

5.作業內容

5.1 資訊安全事件之管理

5.1.1 應建立處理資訊安全事件之作業程序，並賦予相關人員必要的責任，以便迅速有效處理資訊安全事件。

5.1.2 發生資訊安全事件之反應與處理作業程序，應納入下列事項：

5.1.2.1 電腦當機及中斷服務。

5.1.2.2 資訊系統環境遭入侵或破壞。

5.1.2.3 業務資料不完整，或資料不正確導致的作業錯誤。

5.1.2.4 機密性資料遭侵犯。

5.1.3 除正常的應變計畫外（如系統及服務之回復作業），資訊安全事件之處理程序，尚應納入下列事項：

5.1.3.1 導致資訊安全事件原因之分析。

5.1.3.2 防止類似事件再發生之補救措施的規劃及執行。

5.1.3.3 電腦稽核軌跡及相關證據之蒐集。

5.1.3.4 與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。

5.1.4 電腦稽核軌跡及相關的證據，應以適當的方法保護，以利下列管理作業：

5.1.4.1 作為研析問題之依據。

5.1.4.2 作為研析是否違反契約或是違反資訊安全規定的證據。

5.1.4.3 作為與軟體及硬體之供應商，協商如何補償之依據。

5.1.5 應以審慎及正式的行政程序，處理資訊安全事件。作業程序應該包括下列事項：

5.1.5.1 應在最短的時間內，確認已回復正常作業的系統及安全控制系統，是否完整及正確。

5.1.5.2 應向管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。

5.1.5.3 應限定只有被授權的人員，才可使用已回復正常作業的系統及資料。

5.1.5.4 緊急處理的各項行動，應予詳細記載，以備日後查考。

5.2 資訊安全事件之通報

5.2.1 若發現或懷疑有資訊安全事件時，應依「資訊-程序-23 資訊安全事件通報及危機處理程序書」訂定的通報管道，迅速通報權責主管單位及人員立即處理。

5.2.2 員工及與本校簽訂保密協議的外部人員，皆應明確告知各種資訊安全事件的反應及報告程序，使其瞭解相關的處理程序。

5.3 資訊安全弱點之反映

5.3.1 應隨時注意資訊系統或資訊服務施設內部之安全弱點、可能面臨的威脅，並迅速告知主管。

5.3.2 系統安全上的弱點，應由專業人員陪同處理，不應任由系統使用者自行修正。

5.4 軟體功能不正常之反映

5.4.1 使用者發現軟體功能有異常時，應迅速告知權責單位或是服務廠商處理。

5.4.2 應建立軟體功能不正常之反映及處理程序：

5.4.2.1 注意螢幕上出現的徵兆或訊息。

5.4.2.2 立即停止使用電腦，迅速通知權責單位。

5.4.2.3 檢視軟體功能不正常的設備，再次啟動前，應以離線方式處理。

5.4.2.4 在任何狀況下，使用者不應自行移除功能不正常的軟體；系統回復作業應由受過適當訓練及有經驗的人員執行。

5.5 檢討作業

5.5.1 應針對已發生且解決之安全事件，於事後檢討何處須再加強安全預防程序。

5.5.2 權責單位應定期向資訊安全長提報資訊安全事件彙總資料，並詳細說明資訊安全管理系統之實施狀況。

6.附件

無。