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-08	文件名稱	矯正及預防管理程序書	
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

為矯正資訊安全管理制度（ISMS）於運作過程中實際發生之缺失與預防潛在之風險，而對相關單位所提出之矯正及預防措施有一適切之管理，以防止類似事件發生達成持續改善之目標，特訂定本程序書。

2.適用範圍

凡本校相關單位執行 ISMS 各項作業所發生之缺失矯正及風險預防等相關措施之管理，均適用本程序書。

3. 參考文件

3.1 資訊-程序-01 文件與資料管理程序書。

4.名詞定義

4.1 潛在風險

指由適當的資料來源，例如影響資訊安全的服務、內部稽核的結果、資訊安全記錄等等，所找出來的潛在問題。目前尚未發生但未來有可能發生之不確定事件。

4.2 矯正

依據實際問題進行檢討與分析，並研擬出改善方案，以矯正發生之缺失。

4.3 矯正措施

為防止不符合 ISMS 實施、操作及使用之事項重複發生，所採取之措施。

4.4 預防

應用適切的資訊來源，以發覺、分析及消除不符合事項之潛在原因。

4.5 預防措施

為預防不符合 ISMS 實施、操作及使用之事項發生，所採取消除未來不符合事項發生之措施。

5.作業內容

5.1 矯正與預防措施管理流程圖

流程	權責單位	相關文件
發現缺失或風險	發現人員	矯正及預防處理單
研擬矯正預防措施	問題發生單位	矯正及預防處理單
審查（No：回研擬矯正預防措施）	單位主管	矯正及預防處理單
Yes		
執行矯正預防措施	問題發生單位	
確認（No：回執行矯正預防措施）	單位主管/執行秘書	矯正及預防處理單
Yes		
維護相關程序	相關單位	
提供管理審查	資訊安全工作小組	矯正及預防處理單
紀錄保存		

5.2 發現缺失或風險

若有需列入管制以避免影響資訊安全管理系統之缺失或風險發生時，發現人員應將異常狀況登錄於「資訊-程序-08-01 矯正及預防處理單」，會辦發生之單位，一般常見之狀況如下。

5.2.1 進行外部稽核發現不符合項目或缺失時。

5.2.2 發生資訊安全事件(含重大異常事件)無法立即進行問題之矯正與處理時及自行發現缺失時。

5.2.3 違反本校資訊安全政策之狀況。

5.2.4 資訊安全目標一直無法達成。

5.2.5 進行資安日常管理及各種資料分析發現異常時。

5.2.6 管理審查提出之改善事項。

5.2.7 其他各項需矯正及預防之狀況。

5.3 研擬矯正預防措施

5.3.1 缺失發生單位於接獲「資訊-程序-08-01 矯正及預防處理單」後，應進行原因分析及評估其影響程度，決定優先順序與處理時限，並研擬矯正預防之改善對策，以確實解決異常狀況。

5.3.2 評估矯正預防措施時，須考慮成本效益及可行性。

5.4 審查

缺失發生單位將「資訊-程序-08-01 矯正及預防處理單」之矯正預防措施送交單位主管審查後執行。

5.5 執行矯正預防措施

缺失發生單位研擬矯正預防之改善對策後，單位主管應指派及督導相關人員負責執行，必要時得協調其他單位予以適當協助，以妥善執行各項矯正預防改善對策。

5.6 確認

缺失發生單位之矯正及預防措施完成改善後，應將結果記錄於

「資訊-程序-08-01 矯正及預防處理單」，呈送單位主管及執行秘書審核，若單位主管或執行秘書不滿意改善結果，則應研擬其他改善措施，持續改善直至改善措施已獲得妥善處理為止。

5.7 維護相關程序

各項矯正及預防措施之改善結果，若有牽涉到資訊安全管理系統之相關程序作業改變，應依「資訊-程序-01 文件與資料管理程序書」之規定，進行相關程序及標準文件之修改。

5.8 提供管理審查

5.8.1 單位主管應於檢討會議中進行各項矯正及預防措施的追蹤及查核，以確保各項矯正與預防措施確實被執行。

5.8.2 各項矯正及預防措施之改善結果，資訊安全工作小組應於管理審查會議前，彙總「資訊-程序-08-01 矯正與預防處理單」之執行狀況，提報管理審查會議。

6.附件

6.1 資訊-程序-08-01 矯正及預防處理單。