管理系統文件

文 件 類 別	第 二 階 文 件	
文 件 編 號	IMS-P-008	
文 件 名 稱	矯正預防及持續改善管理程序書	
發 行 單 位	國立虎尾科技大學	
發 行 日 期	112 年 08 月 23 日	
版　　次	3.0	
適用單位/範圍	全校 (凡業務涉及個資蒐集、處理、利用之單位皆適用之)	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
2.0	108/08/21	因應資通安全管理法施行修訂相關用詞及規範。(6.2.13)
2.1	110/03/29	(1) 3.參考文件刪除「附錄 A 資通安全管理規範」，增訂「國際標準資訊安全管理系統(ISO27001：2013)」。 (2).修訂「6.2 發現缺失或風險」部分內容為:「缺失發現人員應將異常狀況登錄於「IMS-P-008-01 矯正及預防措施處理單」，並提報 IMS 推動小組確認缺失情形後，」。
3.0	112/08/23	因應本校內部流程修訂流程圖及條文內容，修訂條文內容為：5.1、5.2、5.3、6.2、6.2.2、6.2.7、6.2.11、6.2.13.1、6.2.13.3、6.3.1、6.3.2、6.3.3、6.4、6.4.1、6.4.2、6.5、6.5.1、6.5.2、6.5.3、6.5.4、6.5.5、6.5.6、6.5.7、6.6、6.6.1、6.6.2、6.9、6.9.1、6.9.2 及 6.10

1. 目的
為使本校矯正及預防資安及個資保護管理制度（IMS）於運作過程中實際發生之缺失與潛在之風險，而對相關單位所提出之矯正及預防措施有一適切之管理，以避免及防止不符合事項再度發生，達成持續改善之目標。

2. 適用範圍
本校各單位執行資安及個資保護管理制度(IMS)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。

3. 參考文件

3.1. 國際標準資訊安全管理系統(ISO27001：2013)。

3.2. 英國國家標準個人資訊管理系統(BS10012：2017)」。

3.3. 教育體系資通安全暨個人資料管理規範。

3.4. IMS-P-001 文件與紀錄管理程序書。

4. 名詞定義

4.1. 潛在風險
泛指藉由適當的資料來源，例如影響個人資料蒐集、處理及利用的服務、內部稽核的結果、個人資料使用、執行紀錄等等，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
為消除現存之不符合本制度要求或造成資安及個資保護管理事件的原因，防止再度發生所採取的措施。

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

為防止潛在不符合本制度要求或可能影響資安及個資保護管理之原因所採取的措施。

4.6. 持續改善
使資安及個資保護管理制度持續有效性，所採取的各項持續管理措施。

5. 權責

5.1. 待改善事項提出人員
負責填寫「IMS-P-008-01 矯正及預防措施處理單」，將所發現的待改善事項具體陳述與記錄，並送交改善措施權責單位進行後續之矯正與預防工作。

5.2. 改善措施權責單位

5.2.1. 協助單位內資安及個資保護管理事件之矯正與預防工作。

5.2.2. 研擬、執行及追蹤矯正與預防措施工作。

5.3. 改善措施權責主管

5.3.1. 審查及確認矯正與預防措施的執行成效。

5.3.2. 督導單位內對於資安及個資保護管理之矯正與預防工作。

5.4. 資安及個資保護管理小組
將矯正與預防措施之改善狀況，提報本校「資通安全暨個人資料保護推動委員會」審查。

5.5. 資通安全暨個人資料保護推動委員會
審查矯正與預防措施之改善狀況是否已達改善目標。

6. 作業內容

6.1. 矯正預防及持續改善管理流程

作業流程	權責單位	相關表單
發現待改善事項	待改善事項提出人員 (以下簡稱提出人員)	矯正及預防措施處理單
研擬矯正預防措施	改善措施權責單位	矯正及預防措施處理單及佐證資料
審核 (No)	改善措施權責主管	矯正及預防措施處理單
執行矯正預防措施 (Yes)	改善措施權責單位	矯正及預防措施處理單
審核 (No1 / No2)	提出人員 改善措施權責主管	矯正及預防措施處理單及佐證資料
確認 (No)	稽核小組 執行秘書	矯正及預防措施處理單
維護相關程序 (Yes)	相關單位	矯正及預防措施處理單
提供管理審查	IMS 推動小組 資通安全暨個人資料保護推動委員會	矯正及預防措施處理單及佐證資料
追蹤執行狀況	改善措施權責單位 電子計算機中心	矯正及預防措施處理單
記錄保存	改善措施權責單位 電子計算機中心	

6.2. 發現待改善事項

待改善事項提出					
提出日期		提出單位			
屬性	□資通安全保護事項(ISMS)　□個人資料保護事項(PIMS)				
分類	□主要不符合事項　□觀察事項 □次要不符合事項　□建議事項 □資安事件通報　□其他		來源	□內部稽核　□外部稽核 □資安事件　□自行提出 □其他：＿＿＿＿＿＿＿＿	
問題描述 (請依人、事、時、地、物詳述)					
提出人員		資安/個資 專責人員		權責單位 資安/個資窗口	

本校同仁於執行各項業務，若發現有需列入管制以避免影響資安及個資保護管理制度之待改善事項發生時，待改善事項提出人員應將異常狀況登錄於「IMS-P-008-01 矯正及預防措施處理單」，並提報 IMS 推動小組確認缺失情形後，交由改善措施權責單位進行後續處置作業，一般常見之異常狀況如下：

6.2.1. 資安及個資保護管理內部及外部稽核發現不符合事項或缺失。

6.2.2. 發生資安及個資保護資料或檔案遭受竄改、竊取事件。

6.2.3. 違反本校資安及個資保護管理政策之狀況。

6.2.4. 資安及個資保護目標一直無法達成。

6.2.5. 資安及個資保護管理制度管理審查會議所提出之改善事項。

6.2.6. 風險評估結果被列為不可接受風險之個人資料。

6.2.7. 新識別的資通系統及個人資料風險不符合資安及個資保護管理制度事項。

6.2.8. 未遵循相關法律要求。

6.2.9. 上級機關或本校利害關係人所提出的改善事項。

6.2.10. 當事人權利行使或抱怨事件處理不善。

6.2.11. 資通系統和個人資料業務委外管理監督不周事件。

6.2.12. 其他未符合資安及個資保護管理制度需採矯正及預防措施之事項。

6.2.13. 資通安全維護計畫實施情形之稽核結果應提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形：

6.2.13.1. 待改善之項目及內容。

6.2.13.2. 發生原因。

6.2.13.3. 為補強待改善項目所採取管理、技術、人力或資源等層面之措施。

6.2.13.4. 改善措施之預定完成時程及執行進度之追蹤方式。

6.3. 研擬矯正與預防措施

研擬改善對策						
原因分析						
矯正措施	暫時性對策：(控制不符合事項的擴大或消除單一事件的影響)				預計完成日	
預防措施	長期性對策：(消除不符合事項或潛在風險的根本原因，防止類似事件發生)				預計完成日	
權責單位處理人員		權責主管 (行政單位須陳核至一級主管)		審核意見		

6.3.1. 改善措施權責單位於接獲「IMS-P-008-01 矯正及預防措施處理單」後，應針對缺失發生原因進行分析及評估其影響程度，決定優先

順序與處理時限，並研擬矯正與預防之改善對策，以確實解決異常狀況。

6.3.2. 改善措施權責單位應將研擬矯正預防之改善對策及處理情形，記錄於「IMS-P-008-01 矯正及預防措施處理單」中列管，並呈核單位權責主管審核改善對策之合理性。

6.3.3. 評估矯正預防措施時，應考慮人力、時間、經費、成本效益及可行性等因素，以評估矯正與預防措施實施之可能性。

6.4. 矯正措施執行及確認

6.4.1. 改善措施權責單位評估後依據研擬矯正措施執行矯正作業。

6.4.2. 依據擬定矯正措施及矯正執行情況，確認執行效果。

6.5. 審核

評估改善效果					
執行情形	□完成矯正措施 (實際完成日期：_____) □完成預防措施 (實際完成日期：_____)				
	執行細節及自行評估說明：				
權責單位處理人員		提出人員		提出人員審核意見	
權責主管 (行政單位須陳核至一級主管)			權責主管審核意見		
稽核小組		執行秘書		結案意見	□准予結案 □重新對策 (結案日期：_____)

6.5.1. 矯正預防措施的執行情況應會辦待改善事項提出人員，以確認改善過程及結果的妥適性。

6.5.2. 若待改善事項來源為外部稽核或上級機關稽核產生者，則待改善事項提出人員，應向外部稽核委員確認相關改善措施及效果，進行意見回復及簽署作業。

6.5.3. 經待改善事項提出人員回覆簽署審核意見後，改善措施權責單位提交執行情況送交單位權責主管審核。

6.5.4. 改善措施權責主管對缺失矯正情況進行審核，以確保矯正改善結果之有效性。

6.5.5 若改善措施權責主管認為改善結果不佳、確認無法達到預期目標或無法完成矯正作業，則改善措施權責單位應研擬其他改善措施，持續改善直至待改善事項已獲得妥善處理。

6.5.6 改善措施單位若是因故無法於預定時間內完成，但確認矯正措施之成效是完善可完成的，則應請改善措施單位於執行細節補充敘述說明原由。

6.5.7 若權責單位處理人員及權責主管確認待改善之項目及內容是無法執行改善時，應於開立之「矯正及預防措施處理單」對策執行細節填寫相關因應措施或是風險處理形式(如:接受風險、轉移風險、避免風險……等)。

6.6. 執行矯正與預防措施要求

6.6.1. 改善措施權責單位對於所採取之矯正與預防措施，應留下採取措施結果之紀錄，並對相關風險重新評估，以確認其效果。

6.6.2. 矯正與預防措施執行工作由各單位權責主管進行督導，各單位人員並確實記錄及追蹤其改善情形，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。

6.7. 維護相關程序

6.7.1. 若處理單位所提出之矯正與預防措施內容確實有效後，應提出修（制）訂相關管理文件或資料的要求，以維持對策的持續有效。

6.7.2. 各項矯正與預防措施之改善結果，有牽涉到管理制度之相關程序作業改變，應依「IMS-P-001 文件與紀錄管理程序書」之規定，進行相關程序及標準文件之修改。

6.7.3. 矯正預防及持續改善工作內容應納入教育訓練課程。

6.8. 提供管理審查

6.8.1. 本校「IMS 推動小組」應將矯正與預防措施之改善狀況，提報本校「資通安全暨個人資料保護推動委員會」審查。

6.8.2. 各項矯正與預防措施之改善結果，「IMS 推動小組」應於管理審查會議前，彙總「IMS-P-008-01 矯正及預防措施處理單」之執行狀況，提報資安及個資保護管理審查會議。

6.8.3. 主管應於檢討會議中進行各項矯正與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。

6.9. 追蹤執行狀況

6.9.1. 矯正措施之執行狀況，應由改善措施權責單位依據「矯正及預防措施處理單」確實執行。

6.9.2. 改善措施權責單位最遲應於收到「矯正及預防措施處理單」後，應依據所提預計完成日期進行進度管制並記錄，以利有效控管執行情況。

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	矯正及預防措施處理單	各單位(正本) 電子計算機中心(副本)	至少 3 年

7. 相關表單

7.1. IMS-P-008-01 矯正及預防措施處理單。