1. **作業流程圖：**

**矯正及預防管理作業程序**



1. **作業程序：**
   1. 發現缺失或風險

若有需列入管制以避免影響管理制度之缺失或風險發生時，缺失發現人員應將異常狀況登錄於「ISMS-P-008-01 矯正及預防處理單」中，一般常見之異常狀況如下：

* + 1. 進行內部、外部稽核發現不符合事項或缺失時。
    2. 發生資訊安全事件（含重大異常事件），問題無法有效矯正與處理時及自行發現缺失時。
    3. 違反本校資訊安全政策之狀況。
    4. 資訊安全目標一直無法達成。
    5. 進行各種資料分析發現異常時。
    6. 管理審查所提出之改善事項。
    7. 其他各項需矯正及預防之狀況。
  1. 研擬矯正預防措施
     1. 缺失發生單位於接獲「ISMS-P-008-01 矯正及預防處理單」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，並研擬矯正預防之改善對策，以確實解決異常狀況。
     2. 缺失發生單位應將矯正預防之改善對策及其處理情形，記錄於「ISMS-P-008-01 矯正及預防處理單」中列管，並且持續進行後續之追蹤。
     3. 評估矯正預防措施時，須考慮人力、時間、經費、成本效益及可行性評估矯正預防措施實施之可能性。
  2. 審查

缺失發生單位須將「ISMS-P-008-01 矯正及預防處理單」經缺失發生單位主管評估確認後，提交相關權責主管審查後實施。

* 1. 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。

* 1. 確認
     1. 缺失發生單位之矯正預防措施已完成改善後，應將結果記錄於「ISMS-P-008-01 矯正及預防處理單」，呈送權責主管審核。
     2. 若權責主管不滿意改善結果或確認無法達到預期目標，則缺失發生單位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。
     3. 缺失發生單位對於所採取之矯正預防措施，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。
  2. 維護相關程序
     1. 若處理單位所提出之矯正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。
     2. 各項矯正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「ISMS-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。
  3. 提供管理審查
     1. 本校資通安全處理小組應將矯正預防措施之改善狀況，提報本校資通安全管理委員會審查。
     2. 各項矯正預防措施之改善結果，資通安全處理小組應於管理審查會議前，彙總「ISMS-P-008-01 矯正與預防處理單」之執行狀況，提報管理審查會議。
     3. 主管應於檢討會議中進行各項矯正預防措施的追蹤及查核，以確保各項矯正預防措施確實被執行。
  4. 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 | 矯正及預防處理單 | 圖書資訊處 | 至少1年 |

1. **控制重點：**
   1. 為矯正本校資訊安全管理制度（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並達成持續改善之目標。
2. **依據及相關文件：**
   1. ISMS-P-001 文件與紀錄管理程序書
3. **使用表單：**
   1. ISMS-P-008-01 矯正及預防處理單