

國立潮州高級中學

矯正及預防管理程序書

機密等級：限閱

文件編號：CCSH-ISMS-B-014

版 次：1.0

發行日期：110.03.20

修訂紀錄

[illegible]

矯正及預防管理程序書					
文件編號	CCSH-ISMS-B-014	version	1.0	機密等級	限閱

目錄

1 目的.....1

2 適用範圍.....1

3 權責.....1

4 名詞定義.....1

5 作業說明.....2

6 相關文件.....3

矯正及預防管理程序書					
文件編號	CCSH-ISMS-B-014	version	1.0	機密等級	限閱

1 目的

針對國立潮州高中（以下簡稱「本校」）資訊安全管理制度運作過程中發生之不符合事項及潛在之風險，採取相關的矯正及預防措施，以防止類似事件發生，進而達成持續改善之目標。

2 適用範圍

本校資訊安全管理制度各項作業流程發生之不符合事項、發生資訊安全事件及潛在之風險處理事項。

3 權責

3.1 資訊安全委員會：負責矯正與預防措施之管理審查。

3.2 不符合事項權責單位：負責稽核所發現不符合事項、資訊安全事件（含重大異常事件）或自行發現不符合事項之原因分析，決定優先順序與處理時限，提出矯正或預防措施並實施。

4 名詞定義

4.1 矯正措施：為防止不符合資訊安全管理制度實施、操作及使用之事項重複發生，所採取之措施。

4.2 預防措施：為預防潛在不符合資訊安全管理制度實施、操作及使用之事項發生，所採取消除未來不符合事項發生原因之措施。

4.3 不符合事項：不符合資訊安全管理制度實施及操作事項者。依影響程度分為：

4.3.1 主要不符合事項：未執行資訊安全管理制度之要求，或多個次要不符合事項集中於同一控制措施者。

4.3.2 次要不符合事項：未能完全遵循資訊安全管理制度之要求，但為單一事件者。

矯正及預防管理程序書					
文件編號	CCSH-ISMS-B-014	version	1.0	機密等級	限閱

4.3.3 觀察事項：發現可能對資訊安全管理制度造成影響的事實及事件，但未有足夠證據顯示會影響資訊安全政策及目標的達成，卻因未來可能成為不符合事項而需要再覆核。

4.3.4 建議事項：發現可能對資訊安全管理制度造成影響的潛在問題，可提出建議之改善措施，以預防未來發生之可能性。

4.4 潛在風險：尚未發生但未來有可能發生之不確定事件。

4.5 暫時性對策：能控制不符合事項的擴大或消除單一事件的影響之措施。

4.6 長期性對策：能消除不符合事項或潛在風險的根本原因之措施。

4.7 不符合事項權責單位：矯正及預防措施之實際執行單位。

4.8 追蹤人：進行矯正或預防措施執行狀況之追蹤，可由稽核組員、組長或相關權責人員負責，但不可由該矯正或預防措施處理人員擔任。

5 作業說明

5.1 執行時機

5.1.1 內部及外部稽核發現不符合事項時，不符合事項權責單位需提出矯正措施，並填寫於「矯正與預防處理單」。

5.1.2 發生資訊安全事件（含重大異常事件）或自行發現不符合事項時，應執行矯正或預防措施，並填寫於「矯正與預防處理單」。

5.2 原因分析

防制不符合事項權責單位應分析問題發生之原因及影響程度，決定優先順序與處理時限。

5.3 矯正與預防措施評估

5.3.1 不符合事項權責單位提出矯正與預防措施時，得區分為暫時性對策及長期性對策，防止類似事件發生。

5.3.2 評估措施時須考慮成本效益及可行性。

矯正及預防管理程序書					
文件編號	CCSH-ISMS-B-014	version	1.0	機密等級	限閱

5.4 追蹤執行狀況

5.4.1 矯正與預防措施之執行狀況，應由不符合事項權責單位依據「矯正與預防處理單」確實執行。

5.4.2 有關執行狀況之追蹤，由稽核小組組長、組員或相關權責人員負責。

5.4.3 追蹤人最遲應於收到「矯正與預防處理單」後十個工作天內進行首次追蹤，並應於「矯正與預防處理單」上留存追蹤軌跡。

5.5 管理審查不符合事項權責單位應彙整相關矯正及預防措施之執行狀況，於管理審查會議提出報告。

6 相關文件

6.1 矯正與預防處理單