德明財經科技大學

矯正管理規定

機密等級：一般

文件編號：Takming-ISMS-B-014

版　次：V 1.1

初版日期：107.12.25

修　訂　紀　錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	108.09.11	2	執行小組	“矯正與預防處理單”改”觀察、建議及回覆紀錄表”

1. 目的

針對德明財經科技大學(以下簡稱本校)各管理系統運作過程中發生之缺失及潛在之風險，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

適用於本校管理系統各項作業流程發生之缺失及潛在之風險處理事項。

3. 名詞定義

3.1. 矯正

先對不符合項目採取行動以控制並改正，進而處理其後果。

3.2. 矯正措施

判定其發生原因及改善措施，並評估是否有類似不符合項目存在，並據此提出執行改善措施，必要時得考量對管理制度進行變更。

3.3. 外部稽核不符合事項

3.3.1. 主要不符合事項

未執行管理系統之要求，或多個次要不符合事項集中於同一控制措施者。

3.3.2. 次要不符合事項

未能完全遵循管理系統之要求，但為單一事件者。

3.4. 內部稽核不符合事項

查核過程中該項目發現任何缺失，或稽核人員提出需改進事項者，該項目即評為不符合。

3.5. 觀察事項

發現可能對管理系統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。

3.6. 建議事項

發現可能對管理系統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。

3.7. 潛在風險

尚未發生但未來有可能發生之不確定事件。

3.8. 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。

3.9. 永久性對策

能消除不符合事項或潛在風險的根本原因之措施。

4. 權責

4.1. 資訊安全執行小組召集人

負責矯正措施之督導與審查。

4.2. 資訊安全稽核分組

4.2.1. 內部稽核不符合事項提報。

4.2.2. 負責矯正措施之追蹤與彙整。

4.2.3. 於管理審查會議提報矯正措施執行情形。

5. 要求事項

5.1. 矯正措施執行時機

5.1.1. 內部及外部稽核發現不符合事項時，不符合事項處理權責單位需提出矯正措施，並填寫於「觀察、建議及回覆紀錄表」。

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，權責單位應執行矯正措施，並填寫於「觀察、建議及回覆紀錄表」。

5.2. 原因分析與矯正措施評估

5.2.1. 不符合事項處理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。

5.2.2. 提出矯正措施時，得區分為暫時性對策及永久性對策，防止類似事件發生。

5.2.3. 評估措施時須考慮成本效益及可行性。

5.3. 矯正措施追蹤

5.3.1. 矯正措施之執行狀況，應由處理權責單位依據「觀察、建議及回覆紀錄表」確實執行。

5.3.2. 有關執行狀況之追蹤，由各稽核分組人員負責。

5.3.3. 追蹤人員最遲應於收到「觀察、建議及回覆紀錄表」後 30 個工作天內進行首次追蹤，並應於「觀察、建議及回覆紀錄表」上留存追蹤軌跡。

5.3.4. 各稽核分組應彙整相關矯正措施之執行狀況，於管理審查會議提出報告。

6. 參考文件

6.1. 觀察、建議及回覆紀錄表。

6.2. 矯正及預防管理說明書。