德明財經科技大學

矯正及預防管理說明書

機密等級：一般

文件編號：Takming-ISMS-C-009

版　　次：V1.0

初版日期：107.12.25

矯正及預防管理說明書					
文件編號	Takming-ISMS-C-009	機密等級	一般	版次	1.0

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. 目的

德明財經科技大學（以下簡稱本校）為針對資訊安全管理系統(以下簡稱ISMS)運作過程中所發生之缺失及潛在風險，採取相關的矯正及預防措施，避免再次發生類似事件，達成持續改善之目標，特制定「矯正及預防管理說明書」(以下簡稱本說明書)，以資遵循。

2. 適用範圍

本校實施資訊安全管理系統(ISMS) 各項作業流程發生之缺失、發生資訊安全事件及潛在之風險處理事項。

3. 名詞定義

無。

4. 權責

資安執行小組：負責矯正與預防措施之管理審查，就稽核所發現之缺失、資訊安全事件(含重大異常事件)或自行發現缺失之原因分析，決定優先順序與處理時限，提出矯正或預防措施並實施。

5. 要求事項

5.1 執行時機：

內部及外部稽核發現缺失時，缺失權責單位須提出矯正措施，並填寫於「觀察、建議及回覆紀錄表」。

5.2 原因分析：

資訊安全執行小組應責成資訊安全執行分組分析問題發生之原因及其影響程度。

5.3 矯正及預防措施評估：

(1)缺失權責單位提出矯正及預防措施時，得區分為暫時性對策及永久性對策，防止類似事件發生。

(2)評估措施時需考慮成本效益及可行性。

5.4 追蹤執行狀況：

(1)矯正及預防措施之執行狀況，應由缺失權責單位依據「觀察、建議及回覆紀錄表」確實執行。

(2)有關執行狀況之追蹤，由資訊安全執行小組督導權責單位負責。

(3)資安稽核小組最遲應於收到「觀察、建議及回覆紀錄表」後，依據所提預計完成日期進行追蹤，並應於「觀察、建議及回覆紀錄表」上留存追蹤軌跡。

5.5 管理審查：

資訊安全執行小組應彙整矯正及預防措施之執行狀況，於管理審查會議提出報告。

6.參考文件

觀察、建議及回覆紀錄表