

敏惠醫護管理專科學校

「資訊安全管理系統」 營運持續運作管理程序書

機密等級：一般

編號：IS-MHCHCM-02-012

版本編號：1.0

制訂日期：110.12.30

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說 明	核准者
1.0	110.12.30	資訊安全執行小組	初版發行	執行秘書

本程序書由資訊安全執行小組負責維護。

目錄：

1	目的	3
2	適用範圍	3
3	權責	3
4	名詞定義	4
5	作業說明	4
6	相關文件	9

1 目的

1.1 敏惠醫護管理專科學校（以下簡稱本校）為確保營運持續運作，並降低關鍵性業務流程受重大故障或災害之影響，訂定本程序書。

2 適用範圍

2.1 本校相關資訊業務流程。

3 權責

3.1 為使營運持續運作計畫與處理程序能順利執行，維持關鍵業務的持續運作，委由緊急處理小組統籌作業。

3.2 人員若無法於事件發生時執行所賦予任務，則由代理人執行。

3.3 緊急處理小組為任務編組。成員相關權責及作業內容分述如下：

3.3.1 組長：

3.3.1.1 當重大資安事件發生時，負責聯絡、召集緊急處理小組。

3.3.1.2 督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

3.3.1.3 依據事件評估結果，請資訊安全委員會召集人決議是否宣布災變及啟動營運持續運作程序。

3.3.1.4 當災變發生時，配合救災單位指揮搶救人員、物資與設備等工作。

3.3.1.5 負責災後協調指揮清理災害現場。

3.3.1.6 負責規劃營運場所之復原工作。

3.3.2 組員：

3.3.2.1 為各關鍵業務流程負責人。

3.3.2.2 負責召集相關人員，擬定、維護、更新及執行「營運持續運作計畫」及相關災害復原程序。

3.3.2.3 每年負責召集相關人員進行計畫之測試演練。

3.3.2.4 負責營運場所之應變、處理、復原及運轉測試工作。

3.3.2.5 視需要負責災害現場證據收集，俾利訴訟與損害求償事宜。

3.3.2.6 評估損害狀況及執行營運場所之現場復原工作。

4 名詞定義

4.1 無。

5 作業說明

5.1 營運持續運作管理

5.1.1 本校應實施營運持續運作管理作業，結合預防和復原控制措施，將業務災害或故障（如自然災害、意外、設備故障和蓄意行為等）造成的中斷情形降低到可接受的範圍。

5.1.2 應分析業務災害或故障對本校之衝擊，並發展和實施「營運持續運作計畫」，確保能在所需時間內恢復業務運作。「營運持續運作計畫」亦應持續維護並定期演練。

5.2 營運衝擊分析

5.2.1 營運衝擊分析原則

5.2.1.1 針對本校提供之服務，檢視營運業務流程，並依據營運衝擊分析之結果判別出關鍵業務流程。

5.2.1.2 分別判斷各項資訊資產與作業流程中斷，對本校關鍵業務流程之衝擊程度，並考量其影響及最大可容忍中斷時間。

5.2.1.3 各項關鍵業務之運作，若因不可抗力或人為因素，造成服務中斷，應採緊急應變措施及復原程序，以維持日常業務之持續運作，降低對業務活動之衝擊。

5.2.2 營運衝擊分析方法

5.2.2.1 資訊安全委員會針對本校提供之服務，就其業務流程之重要性，依衝擊程度、相關資訊資產之風險、最大可容忍中斷時間(MTPD)、復原時間目標 (Recovery Time Objective, RTO) 與資料復原時間目標 (Recovery Point Objective, RPO) 進行綜合分析，給予「高」、「中」或「低」之分級，並由資訊安全執行小組填寫於「業務流程衝擊分析表」。

5.2.2.2 重要分級為「高」之業務流程，即為本校之關鍵業務流程。

5.2.2.3 關鍵業務流程負責人應對關鍵業務流程擬定「營運持續運作計畫」。

5.3 營運持續運作計畫之內容

5.3.1 營運持續運作計畫應包含下列項目或內容：

5.3.1.1 目的：說明計畫欲達成之目標。

5.3.1.2 中斷狀況：列出關鍵業務流程中較可能出現之中斷狀況。

5.3.1.3 預防措施：說明為預防關鍵業務流程中斷，所做的系統、資料庫之叢集、備援、回復及執行步驟等預防或減災的日常維護措施。

5.3.1.4 事件通報：說明事件通報程序。

5.3.1.5 應變處理：說明災害調查與評估之步驟、臨時指揮中心建置等。

5.3.1.6 回復作業：說明回復場所的清理、清查、準備、人員責任、設施、網路、系統之回復程序等。

5.4 營運持續運作程序測試演練

5.4.1 營運持續運作程序須每年測試演練，以確保計畫之有效性，並使相關人員確實瞭解計畫之最新狀態。測試計畫得以定期測試個別計畫之方式進行。

5.4.2 營運持續運作程序測試前，關鍵業務流程負責人應填寫「營運持續運作計畫演練活動紀錄」之「演練規劃表」，安排規劃與執行事宜。關鍵業務流程負責人視需要得要求相關業務單位協

助。

5.4.3 「演練規劃表」經資訊安全委員會核可後進行測試作業。測試之方式得依實務需求，採下列任一方式進行：

5.4.3.1 檢查表測試 (Check list tests)：提供檢查表予相關人員檢視程序內容，並視實際狀況提出修正建議。

5.4.3.2 書面測試 (Walk-through tests)：集合相關人員共同檢視營運持續運作程序。

5.4.3.3 模擬測試 (Simulation tests)：以模擬環境進行營運持續運作程序測試。

5.4.3.4 完全測試 (Full interruption tests)：於實際作業環境中進行營運持續運作程序測試。

5.4.4 營運持續運作程序測試結果應紀錄於「營運持續運作計畫演練活動紀錄」之「演練暨處理執行表」。

5.5 營運持續運作計畫之更新

5.5.1 「營運持續運作計畫」應視業務、本校及人員的調整需求而定期更新，以確保計畫之有效性。

5.5.2 「營運持續運作計畫」更新之需求，得考量以下事項：

5.5.2.1 採購新設備或更新作業系統。

5.5.2.2 使用新的問題偵測及控制技術（如火災偵測）。

5.5.2.3 人員及組織上之調整變動。

5.5.2.4 部門及辦公場所之變動。

5.5.2.5 契約當事者或供應商之調整變動。

5.5.2.6 應用系統的變動、新建或停用。

5.5.2.7 實務作業的變更。

5.5.2.8 法規上的變更。

5.5.3 關鍵業務流程負責人負責「營運持續運作計畫」變更事宜，

「營運持續運作計畫」每年至少應檢討評估一次，並將檢討與更新的結果送資訊安全委員會核定。

5.6 營運持續運作程序之啟動及結束

5.6.1 關鍵業務流程發生中斷時，關鍵業務流程負責人應進行復原時程評估，若所需復原時程大於復原時間目標（RTO）時，應通知緊急處理小組組長，並由緊急處理小組組長建請召開資訊安全委員會，討論啟動營運持續運作程序事宜。

5.6.2 緊急處理小組組長應儘速將災害現場搶救情況與評估之損失彙整，並呈報資訊安全委員會。

5.6.3 緊急處理小組組長應適時向資訊安全委員會報告關鍵業務流程中斷之處理進度。

5.6.4 重大災害發生造成嚴重損失時（如火災、爆炸、地震、颱風

等)，得不經損害評估，逕行啟動營運持續運作程序。

5.6.5 關鍵性業務流程回復至原始狀態，經確認運作無異常後，緊急處理小組組長應建請召開資訊安全委員會，討論是否結束營運持續運作程序。

5.7 災害現場蒐證與清理

5.7.1 災害現場搶救完成後，緊急處理小組需指派相關人員進行災害現場鑑識與蒐證工作，以做為日後訴訟索賠之依據。鑑識蒐證工作如有需要，應配合相關單位（如消防單位、警察單位等）進行。鑑識蒐證完成後，始可進行現場清理。

5.8 事件處理檢討

5.8.1 事件處理完成後，緊急處理小組須召開檢討會議。檢討事件通報、應變處理與復原作業各階段運作是否達成本程序預定目標，並依據「矯正及持續改善管理程序書」辦理。檢討結果呈報資訊安全委員會，並做為修訂「營運持續運作管理程序書」的重要依據。

6 相關文件

6.1 營運持續運作計畫演練活動紀錄。

6.2 業務流程衝擊分析表。

6.3 營運持續運作計畫。