德明財經科技大學

資訊安全營運持續管理規定

機密等級：一般

文件編號：Takming-ISMS-B-015

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	114.02.08		推動小組	補充名詞定義，”執行”改”推動”，”分組”改”小組”

1. 目的

為防止德明財經科技大學(以下簡稱本校)資訊業務活動中斷，保護關鍵性資訊業務流程不受重大資安事故的影響，擬定關鍵性資訊業務流程遭受重大資安事故時，可執行之替代方案，以確保員工安全與業務的持續運作，降低事件所造成的損失，並作為業務持續計畫發展與維護的依據。

2. 適用範圍

本校資訊關鍵性業務流程。

3. 名詞定義

3.1. 復原目標點(Recovery Point Objective，RPO)
系統中斷期間，可接受在最近一次備份後的數據損失量。

3.2. 復原目標時間(Recovery Time Objective，RTO)
系統或業務恢復正常運作所需的最大時間。

3.3. 最大可容忍中斷時間(Maximum Tolerable Period of Disruption，MTPD)
在發生中斷事故時，能夠容忍的最大中斷時間。

4. 權責

4.1. 資訊安全推動小組召集人

4.1.1. 指派關鍵性業務流程主要權責單位及流程負責人。

4.1.2. 審核業務持續計畫內容之適切性。

4.2. 資訊安全推動小組

4.2.1. 規劃業務持續計畫內容，並進行營運衝擊分析。

4.2.2. 協調及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。

4.2.3. 依據事故評估之現況建請資訊安全推動小組召集人決議是否宣布災變及啟動業務持續計畫。

4.2.4. 當災變發生時，配合救災單位負責搶救人員、物資與設備等及現場指揮工作。

4.2.5. 負責災後協調指揮清理災害現場。

4.2.6. 負責規劃原營運場所之現場復原工作。

4.2.7. 每年負責召集相關人員進行計劃之測試演練。

4.3. 各關鍵業務流程負責人：

4.3.1. 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

4.3.2. 負責每年進行計劃之測試演練。

4.3.3. 負責原營運場所或異地備份場所之應變、處理、復原及運轉測試工作。

4.3.4. 負責災害現場證據收集，俾利未來訴訟與損害求償事宜。

4.3.5. 災害現場評估損害狀況及執行原營運場所之現場復原工作。

5. 要求事項

5.1. 營運持續管理要求

5.1.1. 應實施業務持續管理作業，結合預防和復原控制措施，將資安事故或故障(可能是由於自然災害、意外、設備故障和蓄意行為等引起)造成的中斷情形降低到可接受的等級。

5.1.2. 應分析重大資安事故或故障對組織的衝擊，並發展和實施業務持續計畫，確保能在所需時間內恢復營運作業。

5.1.3. 業務持續計畫應持續維護並定期演練。

5.2. 業務持續計畫

5.2.1. 業務持續計畫制訂之目的在防止當發生重大故障或資安事故造成本校資訊資源相關硬體、軟體、網路通信線路或其他周邊設備故障，導致關鍵性資訊業務服務中斷。

5.2.2. 營運衝擊分析(Business Impact Analysis , BIA)

5.2.2.1. 關鍵營運流程分析

5.2.2.1.1. 由資訊安全推動小組針對本校資訊業務所提供之服務，檢視負責之營運業務流程，依業務之重要性，鑑別並分別給「高」、「中」或「低」之關鍵等級，「高」關鍵等級流程即為本校資訊業務之關鍵性業務流程，並提請資訊安全推動小組召集人核定。

5.2.2.1.2. 資訊安全推動小組召集人指派關鍵性業務流程主要權責單位及流程負責人。

5.2.2.1.3. 辨識關鍵性業務流程是否還有次流程、所依賴之流程或系統，如某流程可能有前端與後端流程或系統、網路基礎架構與設施等。

5.2.2.2. 關鍵營運流程中斷之影響

各項業務之運作，若因不可抗力及人為因素，造成服務中斷，替代程序應以最快的速度進行。

5.2.2.3. 衝擊及最大可容忍中斷時間

判斷各項關鍵營運流程對本校資訊業務營運的衝擊程度、關鍵營運流程中斷之影響程度及範圍、判斷復原目標點(Recovery Point Objective，RPO)、復原目標時間(Recovery Time Objective，RTO)及最大可容忍中斷時間(Maximum Tolerable Period of Disruption，MTPD)。

5.2.2.4. 其他替代程序

一旦提供之服務中斷，應採緊急應變措施及復原的程序，以維持日常業務之持續運作，降低對業務活動的衝擊。

5.2.2.5. 營運衝擊分析結果

營運衝擊分析之結果記錄於「關鍵營運流程分級表」。

5.2.3. 業務持續計畫指導綱要

5.2.3.1. 目的

說明計畫擬訂欲達成之目標。

依據業務營運衝擊分析(BIA)結果，建立本校資訊核心業務(以下簡稱本業務)營運持續管理作業之執行方案。確保本業務流程受重大資安事故導致中斷時，協助管理階層以迅速、有效及有組織的方法，確保員工安全與業務回復正常運作。

5.2.3.2. 範圍

說明計畫含括範圍。

適用於本校資訊業務發生重大資安事故導致業務無法持續運作時，因應之執行方案。

5.2.3.3. 計畫假設

說明計畫擬訂時之假設條件。

5.2.3.3.1. 本計畫啟動時，指定之備份場所及備份資源是可用的。

5.2.3.3.2. 原營運與異地備份場所未同時遭受資安事故損毀。

5.2.3.3.3. 業務環境、作業方式、資訊系統與架構有調整時，所需的復原資源已一併調整，對於執行業務持續計畫的準備能維持一致。

5.2.3.4. 計畫發展、維護

說明計畫發展、變更條件與維護之職責。

5.2.3.4.1. 本計畫之規劃、維護工作由本校電子計算機中心負責。

5.2.3.4.2. 本計畫需提供備份回復作業行動的執行步驟，以確保備份回復工作能即時依序執行。

5.2.3.5. 計畫測試/演練

說明計畫測試/演練的項目與執行方式。本計畫每年進行測試/演練，項目由資訊安全推動小組負責規劃，並由相關業務單位擬訂執行計畫，進行測試/演練過程並將結果填寫於「業務永續運作計畫演練活動紀錄表」。

測試/演練項目依實務需求得採用下列任一方式進行：

5.2.3.5.1. 結構化測試 (Structural walk-through)：召集相關單位與人員進行書面模擬處理方式進行討論。

5.2.3.5.2. 檢查表測試(Checklist tests)：發展檢查表，以便相關人員能夠利用此檢查進行測試。

5.2.3.5.3. 模擬測試(Simulation tests)：建立一個模擬的

環境進行測試。

5.2.3.5.4. 完全測試(Full interruption tests)：在實際作業環境中進行測試。

5.2.3.6. 原營運場所

說明目前營運場所位置。

原營運場所為本校電子計算機中心+辦公區域及電腦機房。

5.2.3.7. 異地備份場所

即異地備份場所位置。

5.2.3.8. 臨時指揮中心

說明臨時指揮中心的位置。當發生資安事故時，原營運場所如果無法使用，資訊安全推動小組應先行成立臨時指揮中心，並進行調度作業。

5.2.4. 備份回復策略

5.2.4.1. 備份回復

說明於異地場所備份回復作業方式。

5.2.4.2. 備份回復策略

說明應用系統備份回復作業之策略目標。

5.2.4.2.1. 應變處理的原則係依據最近一次的營運衝擊分析，以回復關鍵等級為「高」之業務為原則，視設備及建築物損害程度決定於原場所或指定之備份場所復原。

5.2.4.2.2. 應變處理時，關鍵等級為「高」之業務需能維持運作；視時間及資源許可，依序回復關鍵等級為「中」及「低」業務之運作。同時應事先與相關單位溝通可能發生的情況。

5.2.4.2.3. 備份回復策略需依據營運衝擊分析之結果，按照主要業務流程之關鍵等級依序復原，詳「關鍵營運流程分級表」。

5.2.4.2.4. 如需較長時間才能重建或回復至正常作業狀態，應建立暫時性的辦公場所及電腦機房，並運作至永久性辦公場所及電腦機房重建完成。

5.2.4.3. 備份回復作業之驗證

5.2.4.3.1. 說明應用系統備份回復作業須經過使用者確認，始可宣告作業完成。

5.2.4.3.2. 各系統備份回復後，資料庫系統負責人應通知相關單位確認資料的正確性，並設法修補所缺之資料，經確認無誤後，始可宣告回復

作業完成。

5.3. 業務持續計畫之啟動

5.3.1. 資訊安全推動小組對資訊安全事件之影響，進行研判及通知資訊安全推動小組召集人。

5.3.2. 資訊安全推動小組召集人連絡召集資訊安全推動小組，並協調及督導各關鍵業務流程負責人執行作業。

5.3.3. 由關鍵業務流程負責人召集相關人員進行復原時程評估，若所需復原時程大於 RTO 時，通知資訊安全推動小組召集人，並由召集人建請召開資訊安全推動小組討論是否啟動業務持續計畫。

5.3.4. 重大資安事故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，逕行啟動業務持續計畫。

5.4. 營運持續應變處理指導原則

5.4.1. 資安事故應變

5.4.1.1. 說明資安事故應變處理方式，以保護生命及財產安全為首要目標。

5.4.1.2. 資安事故狀況調查，一旦現場可以開放進入，應進入現場評估服務中斷的時間，如果現場不允許進入，除了服務中斷的時間外，應一併評估何時可進入現場進行損害評估及證據保存，評估結果應立即通報資訊安全推動小組。

5.4.1.2.1. 人員狀況

A. 單位主管負責確實清點所屬人員傷亡名單。

B. 人員疏散後，按指定集合地點集合，並由單位主管清點人員後，回報資訊安全推動小組。

5.4.1.2.2. 電腦機房狀況(含牆壁、高架地板及管線)

A. 機器設備之移位件數。

B. 機器設備掉落、傾倒或傾斜數與天花板、高架地板及牆壁塌落面積。

C. 建築物結構狀況。

D. 電腦硬體與網路設備狀況。

E. 相關設備狀況(包括電源、不斷電設備、冷氣及供水等設備)。

F. 儲存媒體狀況(如磁帶、磁片等)。

G. 程式原始碼存放地點狀況。

H. 各系統文件存放地點狀況。

5.4.1.2.3. 辦公場所狀況：

各單位主管清點及回報現況。

A. 電腦硬體與網路設備狀況。

B. 相關設備狀況(包括電源、冷氣、文件、電話及茶水等設備)。
C. 儲存媒體狀況(如磁帶、磁片等)。
D. 各文件存放地點狀況。

5.4.1.3. 資源需求

5.4.1.3.1. 人員、臨時指揮中心及備份場所，或緊急採購等需求。
5.4.1.3.2. 電信通訊聯絡或電子郵件等溝通工具。
5.4.1.3.3. 日常作業程序依各單位標準作業流程辦理。
5.4.1.3.4. 所需之硬體設備規格。
5.4.1.3.5. 所需之軟體規格：作業系統、應用系統、資料庫、自行開發軟體程式碼及網管軟體廠牌、版本、存放位址、使用手冊等。
5.4.1.3.6. 所需之媒體版本、存放位址等。

5.4.1.4. 原營運場所復原

若評估結果可於原營運場所復原，說明復原作業之方式。經資安事故評估可於原場所復原處理，權責單位應立即進行以下工作。

5.4.1.4.1. 電腦系統之復原

A. 先連絡廠商、維護工程師或權責部門，將受損狀況詳加說明。
B. 扶正移位或傾斜之設備。
C. 受損設備更換或維修。
D. 設備個別運轉測試。
E. 系統運轉測試。
F. 系統重開機運轉。

5.4.1.4.2. 相關設備之復原

A. 通知相關單位或廠商，立即維護異常之電源、不斷電系統、冷氣空調及供水等設備。
B. 復原作業速洽有關單位或廠商，以最短時間內完成。

5.4.1.4.3. 儲存媒體之復原

A. 檢查燒損、撞損、破裂、浸水及蒙塵受損程度。
B. 受損輕微可自行清潔者迅速動員處理。
C. 受損致不堪使用者，洽各系統負責人進行補救。
D. 主機、伺服器、作業系統、應用系統、資料庫系統及網路之復原，依據各細部計畫辦理。

5.4.1.5. 對外公開資訊之聯絡說明

向上級長官或對外界說明損害程度及因應對策之職責。資訊安全推動小組應儘速將資安事故現場搶救情況與評估的損失彙整後，提供給資訊安全推動小組召集人負責向上級主管報告，並協助本校發言人對外說明情況與處置方式或向主管機關陳報。

5.4.2. 事後復原

5.4.2.1. 事後復原主要為資安事故現場蒐證、清理、復原、返回原營運場所作業及事件處理檢討。

5.4.2.2. 資安事故現場鑑識與清理

說明資安事故現場搶救完成後，須先經過配合相關單位鑑識蒐證後，方可進行清理與復原。一旦現場可以開放進入，權責單位指派負責人員進行災害現場鑑識蒐證資料收集工作，以做為日後訴訟或保險索賠之依據。鑑識工作應配合相關單位(如：消防單位、警察單位等)進行，鑑識蒐證作業應包含實體與電子部份。蒐證工作完成後，始可進行資安事故現場清理，通知資訊安全推動小組協調相關單位處理。

5.4.2.3. 原營運場所復原

說明原營運場所進行復原的方式、復原作業完成後須進行驗證及切換回原營運場所作業的做法。上述工作完成後，在資訊安全推動小組召集人的指揮下進行復原作業，需於原營運場所先執行營運測試，完成後始可進行恢復作業回復正常營運。

5.4.2.4. 復原規劃作業

由資訊安全推動小組統籌，聯絡相關廠商提供資料，製作規格、編製預算、協辦緊急採購簽案等作業。

5.4.2.5. 執行復原作業

採購完成後，由電腦系統、資料庫、網路通訊、應用系統等各負責人開始執行復原作業，當應用系統復原完成，由相關人員確認復原資料是否正確，並補上資安事故期間處理增加的資料，始可宣告復原作業完成。

5.4.2.6. 返回原作業場所

當各復原作業完成，並經測試作業正常，由資訊安全推動小組召集人宣佈返回原作業場所的時間，並事先請相關單位配合切換作業。切換完成後，備份作業場所即恢復其正常作業。

5.4.3. 事件處理檢討

5.4.3.1. 事件處理完成後，資訊安全推動小組須召開檢討會議。

5.4.3.2. 檢討事件通報、應變處理、備份回復作業、與復原作業各階段運作是否達成本程序預定目標，並依據「矯正管理規定」辦理。

5.4.3.3. 檢討結果呈報資訊安全推動小組召集人，並做為修訂業務持續計畫的重要依據。

5.5. 查證、審查及評估資訊安全持續

5.5.1. 業務持續計畫之測試/演練

5.5.1.1. 業務持續計畫可能會因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，應定期測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需求及頻率。

5.5.1.2. 業務持續計畫須每年進行測試，測試前須填報測試計畫，經核可後進行。測試的方式依實務需求得採用下列任一方式進行：

5.5.1.2.1. 檢查表測試(Checklist tests)
將業務持續計畫發送給相關權責人員，由其檢視計畫並視實際狀況提出修正建議。

5.5.1.2.2. 結構化測試(Structural walk-through)
聚集相關權責人員一起檢視業務持續計畫。

5.5.1.2.3. 模擬測試(Simulation tests)
建立一個模擬的環境進行測試。

5.5.1.2.4. 完全測試(Full interruption tests)
在實際作業環境中進行測試。

5.5.1.3.「業務持續計畫」測試結果應詳實記錄。

5.5.2. 業務持續計畫之更新

5.5.2.1. 業務持續計畫應配合業務、組織及人員的調整變更而定期更新，以發揮計畫的最大投資效益並確保計畫持續有效。

5.5.2.2. 得考量計畫更新之事項如下：

5.5.2.2.1. 採購新的設備，或是更新作業系統。

5.5.2.2.2. 使用新的問題偵測及控制技術(例如火災偵測)。

5.5.2.2.3. 使用新的環境控制技術。

5.5.2.2.4. 人員及組織上的調整變動。

5.5.2.2.5. 部門及人員地址及電話號碼的變動。

5.5.2.2.6. 契約當事者或是供應商的調整變動。

5.5.2.2.7. 應用系統變動、新建或是撤銷應用系統。

5.5.2.2.8. 實務作業的變更。

5.5.2.2.9. 法規上的變更。

5.5.2.3. 資訊安全推動小組負責計畫變更事宜，業務持續計畫每年至少應檢討評估一次，包括執行營運衝擊分析、組織權責與成員之調整、資安事故應變程序及回復策略之檢討，並將年度總檢討與更新的結果向資訊安全推動小組召集人報告。

6. 參考文件

6.1. 資訊資產管理規定。

6.2. 矯正管理規定。

6.3. 關鍵營運流程分級表。

6.4. 業務永續運作計畫演練活動紀錄表。