管理系統文件

文 件 類 別	第 二 階 文 件	
文 件 編 號	IMS-P-006	
文 件 名 稱	業務持續管理程序書	
發 行 單 位	國立虎尾科技大學	
發 行 日 期	112 年 05 月 05 日	
版　　次	2.4	
適用單位/範圍	全校	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
2.0	108/08/21	整合「資通安全管理法」、「資通安全責任等級分級辦法」調整相關程序內容(5.2.1、5.2.2、5.4.2)。
2.1	109/07/06	修改「關鍵業務流程」為「核心業務流程」調整 5.4.2 相關程序內容
2.2	109/08/12	1. 修訂 4.5 中「公司」與「企業」一詞改為「組織」。 2. 修訂 5.7.3 將原有「關鍵業務」一詞改為「核心業務」以符合現況。
2.3	110/03/29	1.修訂「3.1 附錄 A 資通安全管理規範」為:「3.1 英國國家標準資訊安全管理系統(ISO27001：2013)」。 2.刪除原「3.2 教育體系資通安全暨個人資料管理規範」。
2.4	112/05/05	1. 條文 5.7.2.5、5.7.2.6 刪除 2. 修改「核心業務流程」為「關鍵業務流程」

1. 目的

永續運作的目的在於碰到重大意外或造成學校運作中止的突發狀況時，使必要業務得以不受影響持續運行，將其傷害減至最低；所以，為維持施行單位業務的永續運作，應進行相關的規劃及檢測，以達到業務進行不中斷之目標。資通安全量化指標，詳如「IMS-P-005 資安及個資保護目標管理程序書」之規定，以進行資安及個資保護安全目標之管理及確保資安及個資保護管理制度持續有效地進行。

2. 適用範圍

本校關鍵業務流程營運持續計畫(BCP)之規劃、演練與管理。

3. 參考文件

3.1 國際標準資訊安全管理系統(ISO27001：2013)。

3.2 教育體系資通安全暨個人資料管理規範。

3.3 IMS-P-005 資安及個資保護目標管理程序書。

3.4 IMS-P-008 矯正預防及持續改善管理程序書。

3.5 IMS-P-009 資通安全事件管理程序書。

4. 名詞定義

4.1 營運持續計畫(Business Continuity Plans, BCP)

為一書面化的完整流程，主要內容在說明業務中斷事件發生後的應變處理、危機溝通、業務持續與回復正常等作業內容。

4.2 最大可容忍中斷期間(Maximum Tolerable Period of Disruption, MTPD)

資通安全事故發生後，造成關鍵營運流程中斷，關鍵營運流程中所有相關聯之利害關係者所能容忍營運流程中斷之最大可接受時間。

4.3 復原目標時間（Recovery Time Objective, RTO）

資通安全事故發生後，關鍵營運流程中所有相關聯之利害關係者，所期望營運流程中斷復原之時間點。

4.4 資料回復點目標(Recovery Point Objectives, RPO)

資通安全事故發生後，關鍵營運流程中所有相關聯之利害關係者，

可接受資料滅失或遺漏之資料時間差。

4.5 營運衝擊分析(Business Impact Analysis, BIA)
確認組織關鍵業務流程、該流程所需之資源，並且評估流程中斷對組織造成影響程度之分析方法。亦即協助組織鑑別出最長可忍受中斷時間(MTPD)及最快復原目標時間(RTO)，讓組織面對災害時可以降低營運中斷之衝擊、減少營運中斷之成本及時間。

4.6 不斷電系統(Uninterruptible Power Supply, UPS)
在電源中斷時能立刻提供電力，維持電腦系統或是需要電源的精密設備能維持正常運作之系統裝置。

4.7 異地備援機房(Disaster Recovery Site, DR site)
避免資通系統或資料不幸被摧毀、服務停止或中斷時，能夠讓資料快速回復及服務快速啟動，進而讓損失達到最低的備援服務。

4.8 核心業務
公務機關依其組織法規，足認該業務為機關核心權責所在。

4.9 核心資通系統
指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

5. 作業內容

5.1 業務持續管理流程圖

作業流程	權責單位	相關表單
營運衝擊分析	IMS 推動小組	關鍵業務流程分級表
研擬業務持續計劃	IMS 推動小組	
業務持續計劃演練	IMS 推動小組	業務持續計畫＼災害復原演練暨處理報告單
啟動業務持續計劃	IMS 推動小組	
異常分析及檢討	IMS 推動小組	
更新業務持續計劃	IMS 推動小組	
紀錄保存	IMS 推動小組	

5.2 營運衝擊分析

應分析重大災害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。業務持續計畫應持續維護並定期演練。

5.2.1 關鍵業務流程分析

由「IMS 推動小組」針對本校所提供之服務及核心權責所在，檢視其營運之業務流程，並將營運衝擊分析鑑定之結果紀錄於「IMS-P-006-01 關鍵業務流程分級表」。

5.2.2 核心資通系統鑑定

「IMS 推動小組」應針對支持核心業務持續運作必要之系統，依「資通系統防護需求分級原則」鑑別並分別給予「高」、「中」或「普」之防護需求等級，其防護需求等級為「高」者，即為核心資通系統。

5.2.3 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，應立即採取緊急應變措施及復原（替代）程序，以維持日常業務之持續運作，降低對業務活動的衝擊。

5.2.4 衝擊及最大可容忍中斷時間

分別判斷各項關鍵營運流程對本校營運的衝擊程度，關鍵營運流程中斷之影響程度及範圍為何？判斷最大可容忍中斷期間(MTPD)、復原目標時間(RTO)及資料回復點目標(RPO)。

5.2.5 需指派關鍵性業務流程主要權責單位及流程負責人。

5.3 研擬業務持續計畫

5.3.1 業務持續計畫制訂之目的在防止當發生重大故障或災害造成本校相關硬體、軟體、網路通信線路或其他周邊設備故障，導致關鍵性業務服務中斷。

5.3.2 關鍵業務流程主要權責單位或流程負責人，須負責業務持續計畫之制訂工作。「IMS 推動小組」應審核業務持續計畫內容之適切性。

5.3.3 應實施業務持續管理作業，結合預防和復原控制措施，將災害或

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。

5.4　業務持續計畫之測試/演練

5.4.1　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。

5.4.2　業務持續計畫須定期進行測試，各業務流程鑑別之核心資通系統經權責單位主管核准後進行測試及演練，本校**核心資通**系統每二年需辦理一次。測試前須填報測試計畫，經核可後進行。測試的方式得依實務需求採用下列任一方式進行：

5.4.2.1　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。

5.4.2.2　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。

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

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

5.4.3　業務持續計畫測試結果應詳實紀錄。

5.5　啟動業務持續計畫

5.5.1　資安及個資保護對資通安全事件（資安等級 3 級以上）之影響，進行研判及通知「IMS 推動小組」。

5.5.2　「IMS 推動小組」組長應協調及督導各關鍵業務流程負責人執行作業。

5.5.3　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復原目標時間(RTO)或資料回復點目標(RPO)時，

應由「IMS 推動小組」召開會議討論是否啟動業務持續計畫。

5.5.4 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，逕行啟動業務持續計畫。

5.6 查證、審查及評估資通安全持續

「IMS 推動小組」應定期查證所規畫及實作之資通安全永續運作控制措施，以確保其於不利情況期間可有效運行。

5.6.1 「IMS 推動小組」宜藉由下列方式查證其資通安全管理之永續運作：

5.6.1.1 演練與測試資通安全永續運作流程與控制措施之功能，以確保其與資訊。

5.6.1.2 演練及測試運行資通安全永續運作流程與控制措施之認知及例行作業，以確保其效能與資通安全持續目標一致。

5.6.1.3 資通系統、資通安全流程與控制措施或業務永續運作管理/災害復原管理之流程變更時，宜審查資通安全永續運作措施之有效性。

5.6.2 「IMS 推動小組」應就演練處理狀況視情況召開檢討會議，檢討事件通報、應變處理、備援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「IMS-P-008 矯正預防及持續改善管理程序」之規定執行異常事件之矯正措施。檢討結果呈報「IMS 推動小組」，並做為修訂業務持續計畫的重要依據。

5.7 更新業務持續計畫

5.7.1 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。

5.7.2 得考量計畫更新之事項如下：

5.7.2.1 採購新的設備，或是更新作業系統。

5.7.2.2 使用新的問題偵測及控制技術（例如火災偵測）。

5.7.2.3 使用新的環境控制技術。

5.7.2.4 人員及組織上的調整變動。

5.7.2.5　應用系統變動、新建或是撤銷應用系統。

5.7.2.6　實務作業的變更。

5.7.2.7　法規上的變更。

5.7.3　關鍵業務流程負責人須負責計畫變更事宜，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、災害應變程序及回復策略之檢討，並將檢討與更新的結果提報「資通安全暨個人資料保護推動委員會」。

5.8　業務持續計畫指導綱要

5.8.1　計畫準備

5.8.1.1　計畫擬訂

5.8.1.1.1　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事故和災難事件導致中斷時，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。

5.8.1.1.2　範圍：說明計畫所含括之範圍。
適用於本校電腦機房發生重大故障和災難事件導致本業務無法持續運作時，因應之執行方案。

5.8.1.1.3　計畫假設：說明計畫擬訂時之假設條件。

A. 本計畫啟動時，指定之備援場所及備援資源是可用的。

B. 原營運與異地備援場所未同時遭受災害損毀。

C. 本業務環境、作業方式、資通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。

5.8.1.1.4　計畫發展、維護：說明計畫發展、變更條件與維護之職責。

A. 本計畫之規劃、維護工作由本校負責，並由「IMS 推動小組」負責督導。

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

5.8.1.1.5 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「IMS 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「IMS-P-006-02 業務持續計畫＼災害復原演練暨處理報告單」。

5.8.1.2 原營運場所：說明目前營運場所位置。
原營運場所為本校之辦公區域及電腦機房。

5.8.1.3 異地備援場所：說明異地備援營運場所位置。
備援場所原則上比照原營運場所之實體環境安全管理。（註：需配合上級主管機關執行）

5.8.1.4 臨時指揮中心：說明臨時指揮中心的位置。
當發生災變時，原營運場所如果無法使用，「IMS 推動小組」應先行成立臨時指揮中心，並進行調度作業。

5.8.2 預先防制
本階段之主要工作分為三個部份：災害偵測、災害防範及研擬業務持續計畫。

5.8.2.1 災害偵測：說明災害偵測通報方式，以期於災害發生的第一時間，能夠立即反應處理。所有同仁對於可能演變為災害的事件有偵測的責任，特別是在主要辦公場所或機房發生的事件須特別加以注意。

5.8.2.2 災害防範：詳列各種重大災害的防範與減災措施，以做為平時準備防範之依據。對於可能發生的各種災害，實施災害防範與災害減緩措施，以降低可能帶來的損失，請參見下表：

災害	防範措施	災害減緩措施
水災	▪ 相關電機設備不置於地下室	▪ 地下室防水閘門。 ▪ 確保抽水設備正常運作

火災	▪ 用電不可超載 ▪ 規定人員不可於工作場所抽煙	▪ 火警警報器 ▪ 滅火器
地震	▪ 大樓防震設施	▪ 機房機架固定 ▪ 人員疏散 ▪ 保地震險
爆炸	▪ 加強人員攜入物品檢查 ▪ 保全巡邏	▪ 人員疏散 ▪ 保產物險
資訊處理設施硬體故障	▪ 定期保養檢查 ▪ 建置 HA（High Availability）架構 ▪ 建置異地備援機房 (DR site)	▪ 資料備份
電力供應中斷	▪ 定期檢測 ▪ 雙迴路電力供應	▪ UPS ▪ 柴油發電機
人為惡意破壞或入侵	▪ 實體安全的控管 ▪ 門禁措施 ▪ 通知保全	▪ 要求對方提出識別證明及來訪的事由

5.8.2.3 研擬業務持續計畫：根據營運衝擊分析的結果，研擬相關業務持續計畫，納入應變處理階段，以備於災害發生時做為緊急應變處理之依據。依業務實際需求，由業務單位負責研擬業務持續計畫，經單位主管核准後實施。

5.8.2.4 事件通報

當資通安全事件發生時，則依據「IMS-P-009 資通安全事件管理程序書」之規定，進行通報並處理問題。

5.8.3 應變處理指導原則

主要工作為災害應變處理與評估。

5.8.3.1 災害應變

5.8.3.1.1 災害應變處理

說明災害應變處理方式。以保護生命及財產安全為首要目標。

5.8.3.1.2　災害狀況調查

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「IMS 推動小組」組長。

A. 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「IMS 推動小組」組長。

B. 電腦機房狀況（含牆壁、高架地板及管線）：
應負責及處理下列事項：

(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（如光碟、硬碟等）。

(g) 程式原始碼存放地點狀況。

(h) 各系統文件存放地點狀況。

C. 辦公場所狀況：

(a) 各單位主管清點及回報現況。

(b) 電腦硬體與網路設備狀況。

(c) 相關設備狀況（包括電源、冷氣、文件、電話及茶水等設備）。

(d) 儲存媒體狀況（如光碟、硬碟等）。

(e) 各文件存放地點狀況。

5.8.3.1.3　資源需求

A. 人員、臨時指揮中心及備援場所，或緊急採購等需求。

B. 電信通訊聯絡或電子郵件等溝通工具。

C. 日常作業程序依各單位標準作業流程（SOP）辦理。

D. 所需之硬體設備規格。

E. 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。

F. 所需之媒體版本及存放位址等。

5.8.3.1.4　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。經災害評估可於原場所復原處理，權責單位應立即進行以下工作。

A. 電腦系統之復原：

(a) 先聯絡委外廠商、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。

B. 相關設備之復原：

(a) 通知相關單位或委外廠商，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委外廠商，以最短時間內完成。

C. 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。

5.8.3.1.5 對外公開資訊之聯絡

向上級長官或對外界說明損害程度及因應對策之職責。「IMS 推動小組」組長應盡速將災害現場搶救情況與評估的損失彙整後，提供給資安及個資保護向上級報告，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。

5.8.3.2 備援回復策略

5.8.3.2.1 備援回復

詳細說明於異地場所備援回復作業之方式。業務持續計畫專案負責人依據各業務持續計畫辦理。

5.8.3.2.2 備援回復策略

說明應用系統備援回復作業之策略目標。

A. 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援場所復原。

B. 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。

C. 備援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，詳如「IMS-P-006-01 關鍵業務流程分級表」。

D. 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。

5.8.3.2.3 備援回復作業之驗證

說明應用系統備援回復作業必須經過使用者確認，始可宣告作業完成。各系統備援回復後，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。

5.8.3.3 事後復原

主要為災害現場蒐證、清理、復原、返回原營運場所作業及事件處理檢討。

5.8.3.3.1 災害現場鑑識與清理

說明災害現場搶救完成後，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，始可進行災害現場清理，通知「IMS 推動小組」協調相關單位處理。

5.8.3.3.2 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「IMS 推動小組」組長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。

A. 復原規劃作業

由「IMS 推動小組」統籌，聯絡相關委外廠商提供資料，製作規格、編製預算、協辦緊急採購簽案等作業。

B. 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，由相關單位確認復原資料是否正確，並補上災變期間處理增加的資料，始可宣告復原作業完成。

C. 返回原作業場所

當各復原作業完成，並經測試作業正常，由「IMS 推動小組」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，備援作業場所即恢復其正常作業。

5.9 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	關鍵業務流程分級表	電子計算機中心	至少 3 年
2	業務持續計畫＼災害復原演練暨處理報告單	電子計算機中心	至少 3 年

6. 附件

6.1 IMS-P-006-01 關鍵業務流程分級表。

6.2 IMS-P-006-02 業務持續計畫＼災害復原演練暨處理報告單。