XXXX學校

業務永續運作管理程序書

機密等級：一般

文件編號：XXXX-B-012

版　　次：1.0

發行日期：109.XX.XX

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

業務永續運作管理程序書					
文件編號	XXXX-B-012	機密等級	一般	版次	1.0

目錄

1　目的

XXXX學校（以下簡稱「本校」）為確保本校業務永續運作，並降低關鍵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

本校承辦相關資訊業務服務之關鍵業務流程。

3　權責

3.1　為使業務永續運作計畫與處理程序能順利執行，並維持關鍵業務的持續運作，由緊急處理組統籌負責相關作業。

3.2　緊急處理組為任務編組，其成員相關權責及作業內容分述如下：

3.2.1召集人：

3.2.1.1　當重大資安事件發生時，負責聯絡、召集緊急處理組。

3.2.1.2　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。

3.2.1.3　依據事件評估結果，建請資通安全委員會召集人決議是否宣布災變及啟動業務永續運作計畫。

3.2.1.4　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。

3.2.1.5　負責災後協調指揮清理災害現場。

3.2.1.6　負責規劃原營運場所之復原工作。

3.2.2各關鍵業務流程負責人：

3.2.2.1　負責召集相關人員，擬定、維護、更新及執行「業務永續運作計畫」及相關災害復原程序。

3.2.2.2　每年負責召集相關人員進行計畫之測試及演練。

3.2.2.3　負責原營運場所或資料備援場所之應變、處理、復原及運轉測試工作。

3.2.2.4　視需要負責災害現場證據收集，俾利未來可能之訴訟與損害求償事宜。

3.2.2.5　評估損害狀況及執行原營運場所之現場復原工作。

4 名詞定義

4.1 復原時間目標（Recovery Time Objective, RTO）：於基礎設施正常供應下，關鍵業務從事件發生到復原的目標時間。

4.2 資料復原時間目標（Recovery Point Objective, RPO）：於基礎設施正常供應下，關鍵業務從事件發生到復原期間，資料所能回復之時間點。

5 作業說明

5.1 業務永續運作管理

5.1.1本校應實施業務永續運作管理作業，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）所造成之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組織之衝擊，並發展和實施「業務永續運作計畫」，確保能在所需時間內恢復業務運作。「業務永續運作計畫」亦應持續維護並定期演練。

5.2 業務衝擊分析（Business Impact Analysis, BIA）

5.2.1資通安全小組應針對本校所提供之業務服務，檢視其流程依業務之重要性、資訊資產價值及風險評鑑結果，鑑別出關鍵業務。

5.2.2進行業務衝擊分析，應判斷各項資訊資產與業務流程中斷時，對於本校各項業務流程之影響及衝擊程度，據以判斷最大可容忍中斷時間、復原時間目標（Recovery Time Objective, RTO），以及資料復原時間目標（Recovery Point Objective, RPO）等，分別給予「高」、「中」或「低」之重要分級，並將業務衝擊分析之結果登錄於「業務流程衝擊分析表」，並呈資通安全委員會審查。

5.2.3重要分級為「高」之業務流程，即為本校之關鍵業務流程。

5.2.4資通安全小組應針對鑑別出之關鍵業務指派負責人，各關鍵業務流程負責人應對關鍵業務流程擬定「業務永續運作計畫」。

5.2.5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，應採取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。

5.3 業務永續運作計畫之內容

業務永續運作計畫應包含下列項目或內容：

5.3.1目的：說明計畫欲達成之目標。

5.3.2範圍：說明計畫所含括之範圍。

5.3.3計畫假設：說明計畫擬定時之假設條件。

5.3.4計畫之發展與維護：說明計畫之發展、變更條件與維護之職責。

5.3.5計畫測試及演練：說明計畫測試及演練之項目與執行方式。

5.3.6事件通報：說明事件通報程序。

5.3.7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。

5.3.8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 業務永續運作計畫測試演練

5.4.1業務永續運作計畫須每年測試演練，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業務永續運作計畫測試前，關鍵業務流程負責人應撰寫「關鍵業務障礙偵測與復原作業程序」，並將演練規劃內容填寫於「業務永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」經資通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（Checklist 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業務永續運作計畫。

5.4.3.3 模擬測試（Simulation tests）：以模擬環境進行業務永續運作計畫測試。

5.4.3.4 完全測試（Full interruption tests）：於實際作業環境中進行業

務永續運作計畫測試。

5.4.4業務永續運作計畫測試結果應紀錄於「業務永續運作計畫演練活動紀錄」之「演練暨處理執行表」。

5.5 業務永續運作計畫之更新

5.5.1「業務永續運作計畫」應視業務、組織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「業務永續運作計畫」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「業務永續運作計畫」變更事宜，「業務永續運作計畫」每年至少應檢討評估一次，並將檢討與更新的結果送資通安全委員會核定。

5.6 業務永續運作計畫之啟動及結束

5.6.1關鍵業務流程發生中斷時，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，應通知緊急處理組召集人，並由召集人建請召開資通安全委員會，討論啟動業務永續運作計畫事宜。

5.6.2緊急處理組召集人應儘速將災害現場搶救情況與評估之損失彙整，並呈報資通安全委員會。

5.6.3緊急處理組召集人應適時向資通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，逕行啟動業務永續運作計畫。

5.6.5關鍵性業務流程回復至原始狀態，經確認運作正常後，緊急處理組召集人應建請召開資通安全委員會，討論是否結束業務永續運作計畫。

5.7 災害現場蒐證與清理

災害現場搶救完成後，緊急處理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

事件處理完成後，緊急處理組須召開檢討會議。檢討事件通報、應變處理與復原作業各階段運作是否達成業務永續運作計畫之預定目標，並依據「矯正及預防管理程序書」辦理。相關檢討結果須呈報至資通安全委員會，做為修訂本程序書之重要依據。

6 相關文件

6.1 安全事件管理程序書

6.2 矯正及預防管理程序書

6.3 業務永續運作計畫

6.4 關鍵業務障礙偵測與復原作業程序

6.5 業務永續運作計畫演練活動紀錄

6.6 業務流程衝擊分析表