雲林縣西螺鎮公所

營運持續管理程序

文件編號： XLTG-02-014

版　　次： V1.0

文件日期： 110 年 11 月 24 日

機密等級： 普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
V1.0	110.11.24	初版發行	ISMS 執行小組	

目　　錄

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)為確保重要資訊業務營運服務不受重大資訊系統失效或災害影響，在各項可能中斷業務活動之事故發生後，得以迅速恢復作業，特訂定本「營運持續管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所發生重大資訊安全事故造成損害，使得營運活動無法正常運作時，包含管理權責單位相關人員、資訊處理相關設施與資訊系統等。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 ISMS 執行小組組長審查本程序，並督導本程序之執行。

三、 ISMS 執行小組：

（一）研擬、評估及檢討本程序。

（二）規劃資訊業務營運持續相關計畫。

（三）執行資訊業務災害回復作業測試演練。

（四）災害發生時之應變與處理。

（五）進入災害現場評估災害損害情形。

（六）災害現場證據收集。

四、 ISMS 承辦人協調及彙總本程序之執行。

五、 本所各單位：

（一）配合營運持續管理相關作業之協調。

（二）配合營運持續模擬測試演練。

肆、 定義

一、 針對本所主要資訊設備、應用系統、網路與通信設施及辦公場所，可能造成營運中斷影響之災害，可分為：

(一)內部危安事件，如內部人員作業疏失或惡意破壞毀損等。

(二)外力入侵事件，如病毒感染事件、駭客攻擊或非法入侵事件等。

(三)天然災害，如颱風、水災、地震等。

(四)重大突發事件，如火災、爆炸等。

二、 復原與回復

(一)現場復原（Recovery)：針對整體性之作業復原，包含人員動員、場地整理、設備復原、作業復原確認等。

(二)系統回復（Restore)：執行資訊系統之復原。

三、 預防措施：指可防止災害發生的控制措施。

四、 減災措施：指可減少或避免災害發生所造成損失的控制措施。

伍、 管理項目

為確保重要營運活動不受天然災害、設備故障或遭破壞之影響，本所同仁須於平時進行各項災害預防措施及模擬演練作業，並於災害或事故發生時，迅速採取緊急應變及回復作業，以確保重要資訊業務得以迅速恢復並持續營運。相關作業如下圖 5-1 所示。

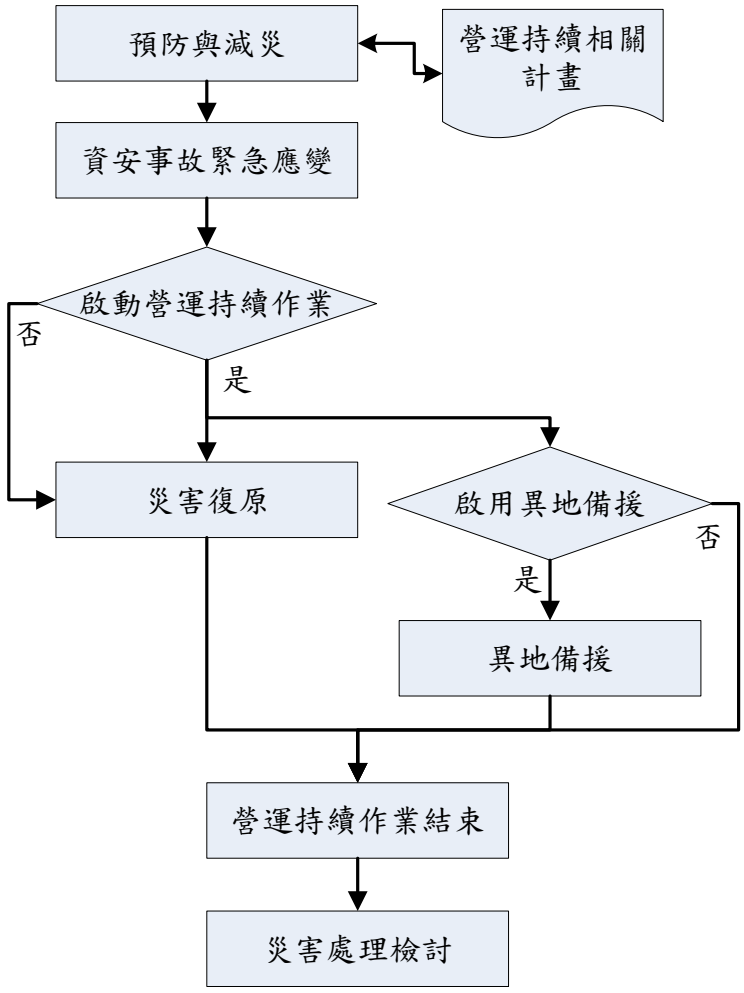

圖 5-1：資訊業務營運持續管理流程圖

一、 預防與減災

（一） 災害防範與減災措施

1. ISMS 執行小組應依據風險評鑑結果，對重要營運活動及可能發生

的各種災害排定優先順序，除給予適當的防護，並實施災害防範與減災措施，以防止或降低災害發生時所帶來的損失。相關災害防範與減災措施可參考附件一、「災害預防與減災措施表」。

2. ISMS 執行小組應建立與維護災害緊急應變任務分工名單(如附件二)，並於實施災害演練時，檢測相關聯絡資料是否正確。

3. ISMS 承辦人每年依「災害預防與減災措施表」，針對各項防範與減災措施辦理檢討，列入資訊業務災害復原作業演練項目。

4. 主機房管理相關人員須定期對機房內之重要設備及資訊系統執行備份與復原測試，相關作業按「備份與回復管理程序」規定辦理。

（二）災害偵測

本所所有人員對於可能演變為災害的事件有偵測及通報的責任，特別是在本所主機房的資訊設施與辦公場所發生的事件須加以注意。若發現災害事故時，應立即按「資安事故管理程序」通報相關單位進行處理。

（三）平日安全防護

會造成營運活動或服務中斷的情況包括：電力中斷、火災、天然災害、設備故障、病毒/駭客攻擊、網路中斷與外力破壞等各種可能因素，ISMS 執行小組平日即應採取各項安全防護措施，並選定適當場所做為備援及災害復原指揮中心，以避免造成營運中斷，滿足營運持續要求。

1. 電力中斷

(1)主機房管理權責單位應評估主機房內所有設備對電力之需求，並預估其成長量及備援電力供應時間，設置不斷電設備

(UPS)。

(2)不斷電設備(UPS)容量應可提供主機房重要設備電源至少半小時以上(滿載時)，以避免電力瞬斷或電壓不穩定時，造成機房內設備停止運轉之情形。

(3)當接獲臺灣電力股份有限公司停電通知時，應由主機房管理權責單位研判是否需配合停機，如需停機，應事先通知本所各單位停止資訊系統服務，並於全球資訊網上公告暫停服務訊息，並由主機房管理相關人員於電力中斷前完成停機相關作業。

2. 火災

(1)主機房內應設置煙霧偵測系統及滅火相關設備，可於火災初期給予有效防護，將可控制之火勢予以撲救（但仍應先通知消防單位以避免火勢失控)。

(2)手提滅火器應置於明顯且易於取得的位置，ISMS 執行小組應規劃及實施消防演練活動。

3. 天然災害

(1)颱風來襲時，應緊閉門窗，做好停電、網路中斷等防範措施。

(2)主機房內設備應安置牢固，以避免地震發生時脫落損壞。

4. 設備故障：對各式設備應定期檢測，以維持其有效性與可用性。

5. 病毒/駭客攻擊

(1)本所資訊系統應安裝防毒軟體及防火牆等安全防護系統，並即時更新至最新之病毒碼。

(2)定期執行漏洞掃瞄及滲透測試，以對資訊系統之漏洞及弱點進行修補。

(3)對於無法修補之漏洞及弱點，應加強安全監控，並採取適當

之控制措施。

6. 外力破壞

(1)落實只有經授權的人員才能進入防護區域，以減少實體破壞的風險。

(2)主機房內外應裝設攝影監視設備，以利萬一遭受破壞時，能調閱錄像資料，追究相關責任。

（四）備援機制

1. 硬體設備替代備援：相關硬體之備援，可於主機房設置備援設備或由委外維護服務廠商提供替代硬體設備。

2. 儲存媒體/磁帶備份：按「備份與回復管理程序」之規定辦理。

3. 職務代理人：各資產及營運作業需建立代理人機制，以利營運持續之實施。

4. 異地備援：ISMS 執行小組應評估資訊系統之營運風險及營運持續需求，決定是否須設置異地備援場所。如需設置時，應依據通訊需求及有時間急迫性之業務，備妥必要設施，以支援營運持續之相關作業。其設備內容應包括：

(1)備援網路設備及網路管理相關主機、應用系統及資料庫等。

(2)對外網路頻寬。

(3)足夠的作業空間。

(4)電話傳真等通訊設備。

(5)安全防護措施。

二、 營運持續相關計畫之制定、維護、測試及演練

為確保災害發生時能立即有效因應，並維持本所資訊系統之基本運作，ISMS 執行小組應研擬營運持續相關計畫，如災害復原計畫、異地備

援計畫等，並定期維護、測試及演練，以確保其有效性，並使相關人員確實瞭解內容的最新狀態。

（一）營運持續相關計畫之制定

「營運持續作業」主要是考量營運衝擊（Business Impact Assessment，BIA）的程度，及最大可容許的失去服務時間（Maximum Tolerable Downtime，MTD）的時間。ISMS 執行小組應依據資產價值分析、風險評鑑結果、以及過往資訊安全事故發生之經驗教訓(lesson learn)等，制訂年度資訊業務營運持續相關計畫，經 ISMS 執行小組組長審查同意後，簽奉資安長核定實施。

（二）營運持續相關計畫之維護

1. ISMS 執行小組每年至少 1 次檢視營運持續相關計畫之適切性及執行成效，並由資安長進行查核，若有任何內容因現行環境或新進威脅而有變更，由 ISMS 承辦人彙整後，陳報 ISMS 執行小組組長，經 ISMS 執行小組組長確認後，指派適當人員進行版本維護更新工作。可能之變更如下：

(1)營運政策的變更。

(2)法規上的變更。

(3)營運面及財務面風險的變更。

(4)業務、組織及人員的調整變動。

(5)實務作業的變更。

(6)場所、設施和資源的變更。

(7)應用系統變動、新建或汰除。

(8)採購新的設備或系統升級。

(9)承包商、供應商和本所人員業務的調整變動。

(10)人員聯絡方式變動。

2. 營運環境發生重大異動且確認對資訊風險有重大影響時，應於完成風險評鑑與管理程序後，依據評估之結果調整營運持續相關計畫。

3. 重要業務流程改變或有重大資安事件通告時，必須檢視營運持續相關計畫，並施予必要之調整。

（三）營運持續相關計畫測試及演練

1. ISMS 執行小組應規劃定期演練年度營運持續相關計畫，並詳實記錄演練測試過程，以評估其可行性及有效性。

2. 訓練不同領域之重要幹部或管理人員，以利相關人員熟悉營運持續啟動時之執行過程。

3. 演練可以定期測試個別項目的方式進行，以減少完整測試所需耗費之人力與資源，可參考下列模式進行：

(1)沙盤推演：針對各種災害情況進行書面流程演練。

(2)狀況模擬：針對各種災害情況，訓練相關人員於災害現場復原時之分工管理，例如通報演練和疏散演練。

(3)完整演練：測試組織、人員、設備、設施和作業均能執行現場復原作業。

4. 演練結果報告應載明以下事項：

(1)演練範圍與項目。

(2)演練時間。

(3)演練地點。

(4)參加演練單位與人員。

(5)演練狀況與處理步驟。

(6)演練結果檢討。

5. 演練結果報告由 ISMS 承辦人彙整，經 ISMS 執行小組組長審查同意後，陳報資訊安全管理委員會。

6. 認知與訓練

(1)ISMS 承辦人應定期針對不同層級人員舉辦危機處理教育訓練，以認知營運持續的重要性。

(2)訓練協助執行本程序中不同領域之重要幹部或管理人員，以利相關計畫能夠依災難特質彈性的進行延伸或變通。

三、 資安事故緊急應變

資安事故發生時之緊急應變處理，相關災害現場搶救及災害評估鑑識作業，按「資安事故管理程序」之規定辦理。

四、 啟動營運持續作業

（一） 當本所發生重大資安事故（如火災、水災、地震、建築物之損害、法定傳染病等），導致主機房、主要資料處理設備、網路通信設施、辦公場所遭受損害或重要資料毀損等，迫使重要服務作業必須中斷，經主機房管理相關人員研判無法在短期內復原時，應通報 ISMS 執行小組組長。

（二） ISMS 執行小組組長於接獲通知後，得邀集相關人員進行研商，決定是否需啟動資訊業務營運持續作業。

五、 營運持續作業

（一） 當 ISMS 執行小組組長決定啟動資訊業務營運持續作業時，ISMS 執行

小組及規劃參與人員應按已選定之場所成立災害復原指揮中心，並按營運持續相關計畫執行各項作業。

（二）如原先選定之災害復原指揮中心預定地點無法使用，ISMS 執行小組應另行尋找適當場所成立災害復原指揮中心。

（三）災害復原指揮中心應依附件三「資源檢核表」所列項目，準備所需物品。

六、 災害復原

（一）ISMS 執行小組針對災害事件造成之結果評估損害情形，以決定適當之復原策略；復原程序採用階段進行方式，由最關鍵之步驟開始進行。

（二）現場復原

1. ISMS 執行小組應協調相關人員清理災害現場。
2. 資訊業務災害復原作業，應依最近一次營運衝擊分析或資產價值評估結果，將資訊系統按其價值或重要性等級循序復原。
3. ISMS 執行小組應針對災害造成之相關資產損壞進行清查，將結果記錄於「損壞資產清冊」，並依清單所列進行相關復原與測試作業。
4. 進行復原作業時，主機房復原順序處理原則如下：

(1)主機房之實體設備相關回復順序：

A. 電力與空調相關之設備為優先。

B. 網路連接相關設備次之。

C. 備援設備回復、資料回復、文件傳送/接收中繼設備等。

(2)主機房之各相關網路實體設備、資料庫、資料之災難回復順

序：

A. 相關網路實體設備為優先。

B. 應用系統程式次之。

C. 資料庫。

D. 資料回復。

5. 資訊系統復原完成後，應由使用單位確認資料之正確性，始得宣告可正常作業。

（三）系統回復

進行系統回復處理時，須於主要備援設備及相關資訊系統設備可運作後，按下列相關處理方式：

1. 單純應用程式(或檔案)損害：由資通安全處理小組之應用系統回復負責人會同各應用系統管理權責單位，備妥回復所需媒體，協調應用系統維護廠商進行應用系統之應用程式(或檔案)回復作業事宜。

2. 資料庫損害：由資通安全處理小組之資料庫系統回復負責人會同各應用系統管理權責單位，備妥回復所需媒體，邀集資料庫之權責單位或系統維護廠商進行資料庫回復作業事宜。

3. 主機或機關網路嚴重損害：由資通安全處理小組之主機系統回復及網路系統復原負責人，協調主機或網路設備相關廠商進行故障修護（或由廠商提供相當的替代設備），將作業系統平台回復至可正常運作狀態，再備妥回復應用系統所需的媒體後，由災害緊急應變任務分工名單各負責人處理後續應用程式、檔案及資料庫回復作業事宜(如前述)。

4. 主機房嚴重損害: 當機房毀損時，須於事前選定之臨時機房替代

地點，重新架設設備及網路環境後，按前述處理方式辦理。

七、 啟用異地備援

（一）當發生緊急事故（如火災、水災、地震、建築物之損害、工程施工、重大疫情等）所造成的服務中斷及損害，由 ISMS 執行小組評估災害嚴重程度，以研判是否需遷移至備援地點。評估原則包括：

1. 災害的特性。

2. 預估中斷的時間。

3. 備援地點的現況。

4. 員工/災害處理人員的情況。

（二）ISMS 執行小組研判原機房所在地點無法在短期內復原使用，有必要遷移至備援地點繼續營運時，由 ISMS 執行小組組長陳報資安長同意後，正式啟動異地備援計畫。

八、 營運持續作業結束

（一）重要資訊服務恢復運轉並維持正常運作後，由該資產之權責單位及管理人進行確認，並將確認結果回報 ISMS 執行小組組長。

（二）ISMS 承辦人將處理結果彙整後報告 ISMS 執行小組組長，確認已恢復正常作業後陳報資安長，並由資安長決定是否宣告災害解除。

（三）資安長決定災害解除後，ISMS 執行小組組長可決定是否結束資訊業務營運持續管理作業，並解散災害復原指揮中心。

九、 災害處理檢討

ISMS 執行小組組長於作業結束後，應召開事件處理檢討會議，討論

該次事件處理流程是否有需要改善之處。

陸、 參考文件

一、 行政院國家資通安全會報「各機關處理資通安全事件危機通報緊急應變作業注意事項」。

二、 資安事故管理程序。

三、 備份與回復管理程序。

柒、 使用表單

損壞資產清冊

附件一、 災害預防與減災措施表

災害	預防措施	減災措施
水災	相關電機設備不置於地下室	● 堆置沙包 ● 準備抽水機
火災	● 規定人員不可於室內抽煙 ● 用電不可超載	● 使用滅火器 ● 疏散人員
重大疫情	● 人員勤洗手消毒等防疫措施 ● 定期健康檢查	● 人員分組輪班
地震	● 人員定期進行防災演練	● 機房機架固定 ● 疏散人員
爆炸	● 加強人員帶入物品檢查 ● 可疑物品檢查	● 疏散人員
資訊處理設施硬體故障	● 定期保養檢查 ● 建置 HA(High Availability)功能 ● 資料備份 ● 簽訂維護合約	● 啟用備援設備
電力供應中斷	● 定期檢查 ● UPS	● 啟用 UPS 電力 ● 啟用(租借)發電機
空調故障	● 定期檢查保養	● 借調強力風扇
網路中毒	● 安裝防毒軟體並即時更新病毒碼 ● 辦理資安宣導講習 ● 規定使用外來資料均先掃毒 ● 不隨便從網路下載檔案	● 中斷中毒區域網路連線 ● 清除或隔離病毒
駭客入侵	● 定期實施弱點掃瞄 ● 即時修補漏洞 ● 安裝及調校防護工具	● 中斷網路連線 ● 向技服中心尋求支援
外力入侵	● 加強衛哨及安全防護 ● 安裝監視設備	● 通知檢.警.調單位處理

附件二、 災害緊急應變任務分工名單

職稱	姓名	角色	職掌	聯絡電話	備註
		■ ISMS 執行小組組長	■ 向資訊安全長報告 ■ 負責啟動與結束資訊業務營運持續作業演練	(O) (H) (M)	
		■ 資通安全處理小組組長	■ 負責收集災害現場資訊及處置狀況 ■ 向 ISMS 執行小組組長報告 ■ 協調及督導各關鍵業務流程復原作業	(O) (H) (M)	
		硬體設備復原負責人	依照計畫進行主機硬體復原之業務	(O) (H) (M)	
		主機系統回復負責人	依照計畫進行主機系統復原之業務	(O) (H) (M)	
		應用系統回復負責人	彙整各應用系統負責人執行應用系統回復狀況	(O) (H) (M)	
		資料庫系統回復負責人	依照計畫進行資料庫系統回復之業務	(O) (H) (M)	
		網路系統復原負責人	依照計畫進行網路回復之業務	(O) (H) (M)	
		儲存媒體負責人	■ 系統異地儲存備份資料 ■ 應用程式及相關資料異地儲存	(O) (H) (M)	
		備援負責人	依照計畫執行復原作業	(O) (H) (M)	
		災害評估負責人	■ 協調相關人員針對災害造成之相關資產之損壞進行清點 ■ 協調相關人員評估災害損害情形	(O) (H) (M)	
		災害鑑識負責人	協調相關人員進行災害現場鑑識蒐證工作	(O) (H) (M)	

附件三、 資源檢核表

所提供之資源		完成準備	
災害急救包	資訊業務營運持續相關表單與電子檔案	□是	□否
	緊急聯絡名單	□是	□否
	資產清冊	□是	□否
	最新風險評鑑表	□是	□否
	資源檢核表	□是	□否
可容納資通安全處理小組成員人數之會議室		□是	□否
白板、白板筆、板擦		□是	□否
大字報用紙		□是	□否
影印機一部		□是	□否
可上網的 PC 或筆記型電腦		□是	□否
印表機一部、A4 紙		□是	□否
辦公用品		□是	□否
網路		□是	□否
電話、傳真機及電話手冊		□是	□否