

環球科技大學

文件名稱	營運持續管理程序	版本	4.0
文件編號	ISMS-02-015	發行日期	2016/10/07
		頁次	1 / 4

1. 目的：

- 1.1 規範圖書資訊處實施資訊安全之永續營運管理作業，結合先期準備和即時矯正處理控制措施，將災害和安全缺失（可能是由自然災害、意外、設備故障、蓄意行為等引起）所造成的服務中斷情形降低至可接受水準。
- 1.2 有效掌握圖書資訊處資通系統遭受破壞或不當使用時，能迅速採取必要的應變措施，在最短時間內復原，以降低該事故可能帶來之損害。

2. 範圍：

有關圖書資訊處資訊機房作業環境。

3. 權責：

3.1 資訊安全組：

- 3.1.1 執行重要系統災害復原及復原後之測試結果。
- 3.1.2 撰寫資訊或個資安全矯正措施報告資料。

3.2 系統（主機）管理員或負責人員：

- 3.2.1 執行重要系統之營運衝擊分析。
- 3.2.2 執行系統災害復原作業。
- 3.2.3 測試系統是否正常提供服務。
- 3.2.4 填寫災害復原演練之相關文件或資料。
- 3.2.5 負責系統維護及更新與修補漏洞。
- 3.2.6 負責系統紀錄與稽核軌跡等證據保全工作。

3.3 內部稽核組：

- 3.3.1 查核系統災害復原之演練過程與結果。
- 3.3.2 查核資訊或個資安全矯正措施實施情形。

環球科技大學

文件名稱	營運持續管理程序	版本	4.0
文件編號	ISMS-02-015	發行日期	2016/10/07
		頁次	2 / 4

4. 名詞解釋：

4.1 營運持續計畫(Business Continuity Plan)：

總括災害復原規劃與組織營運恢復之計畫。

4.2 營運衝擊分析(Business Impact Analysis)：

決定風險分析所辨識出的潛在損失實際上對組織所造成衝擊的後果與嚴重性。營運衝擊分析應盡可能從組織中斷的時間或財務的角度將損失衝擊量化。

4.3 最大允許中斷時間(Maximum Tolerable Downtime)：

組織須維持最低的生產或服務水平，可以允許缺乏關鍵組織服務功能的最大接受時間。

4.4 復原時間目標(Recovery Time Objective)：

組織內主要之服務功能，組織在經營運衝擊分析辨識後所訂定之恢復最低的生產或服務水平目標所需之時間。

4.5 資料回復目標 (Recovery Point Objective)

組織在系統復原後，需進行資料回復的時間。

5. 作業內容：

5.1 營運衝擊分析

5.1.1 圖書資訊處進行營運衝擊分析 BIA (Business Impact Analysis) 時需要考量的條件，包括最大服務中斷時間 MTD (Maximum Tolerable Downtime) 及資料回復目標 RPO (Recovery Point Objective)。鑒於圖書資訊處資訊相關作業特性，對於系統及時回復的需求較高，資料及時復原的需求次之，因此 MTD 幾乎與系統回復時間 RTO (Recovery Time Objective) 相等，本計畫將以 RTO 為主進行說明。

5.1.2 圖書資訊處 RTO 所規範的期間為發生緊急事故至系統服務回復為止。圖書資訊處依四種關鍵服務(提供資訊網路連線服務、提供資訊安全防護服務、設備及伺服器之管理、提供業務資訊化之應用服務)列出重要業務營運衝擊分析如「營運衝擊分析表」。

5.1.3 營運持續分析中如果 RTO 所需要的時間大過於 MTD 的時間，即視為發生事故後，

環球科技大學

文件名稱	營運持續管理程序	版本	4.0
文件編號	ISMS-02-015	發行日期	2016/10/07
		頁次	3 / 4

難以在要求的時間內恢復指定的運作機能，此時，應由資訊安全組成員依照風險評估表中，該資訊資產可能遭遇的威脅作為營運持續發展緊急應變或是災害回復的「情境」。

5.2 系統災害復原執行細則之測試 / 演練

5.2.1 系統災害復原執行細則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，而無法發揮預期作用，應定期測試及演練以確保有效性，並使相關人員確實瞭解內容最新狀態，測試可以定期測試個別項目的方式進行，以減少完整測試的需求及頻率。

5.2.2 系統災害復原執行細則應制訂年度演練計畫(災害復原演練規劃表)，每項演練前填報演練計畫，經陳核組長及圖資長核可後始可進行，每年的演練項目可包括：

5.2.2.1 針對各種情況進行沙盤推演(利用暫時停止營運，以狀況的範例討論災害復原程序)

5.2.2.2 狀況模擬(尤其在意外事件或危機範例後，用以訓練員工的定位管理)。

5.2.2.3 技術性復原測試(以確保資訊系統可有效復原)。

5.2.2.4 測試供應商的設施和服務(以確保廠商提供的服務和產品符合合約中的規定)。

5.2.2.5 完整演練(測試組織、人員、設備、設施和作業是否能夠妥善處理中斷情況)。

5.3.3 演練結果應填寫「測試演練結果報告單」，載明演練部門、參加演練人員、演練日期、起迄時間、演練項目、實際完成時間、演練程序描述及結果檢討，演練結果報告單由負責演練部門提報資訊安全稽核小組確認。

5.4 系統災害復原管理維護及更新

5.4.1 各組應依風險評估結果或災害發生嚴重狀況擬定「災害復原演練規劃表」，並配合圖書資訊處資安相關服務業務、組織及人員的調整變更，進行定期與不定期更新，以確保持續有效。

5.4.2 有進行或變更下列事項時，應更新系統災害復原管理相關紀錄：

5.4.2.1 購買新的設備或更新作業系統。

環球科技大學

文件名稱	營運持續管理程序	版本	4.0
文件編號	ISMS-02-015	發行日期	2016/10/07
		頁次	4 / 4

5.4.2.2 使用新的環境控制技術。

5.4.2.3 人員及組織調整變動。

5.4.2.4 圖書資訊處內部門及人員地址及電話號碼變動時。

5.4.2.5 契約當事人或供應商調整變動時。

5.4.2.6 實際操作流程有變更時。

5.4.2.7 法規上有變更時。

5.4.3 由資訊安全組負責彙整災害復原管理相關資料內容更新維護事宜，如有個別應用系統與資料庫復原程序，應每半年檢討一次災害復原管理相關資料。

5.4.4 完整系統災害復原演練，每年至少操作一次，應包括執行營運衝擊分析、組織權責與成員調整說明、災害應變程序及回復策略之檢討，並將演練結果記錄於「測試演練結果報告單」，再將年度總檢討與更新結果資料簽陳各組組長及圖資長。

6. 相關附件：

無

7. 使用表單：

7.1 營運衝擊分析表 (ISMS-04-042)

7.2 災害復原演練規劃表 (ISMS-04-036)

7.3 測試演練結果報告單 (ISMS-04-043)