德明財經科技大學

關鍵業務障礙偵測與復原作業說明書

機密等級：一般

文件編號：Takming-ISMS-C-005

版　　次：V1.3

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	110.09.16	5	執行小組	新增 5.6 短時間內無法立即解決問題時
1.2	111.05.23	5	執行小組	修訂 5.6 內容
1.3	114.02.08		推動小組	

1. 目的

本說明書乃依據業務衝擊分析（BIA）之結果，建立德明財經科技大學(以下簡稱本校)關鍵業務障礙偵測與復原之作業程序。確保關鍵業務流程於遭受重大事故或災難而導致業務中斷時，協助管理階層以迅速、 有效及有組織之方法，以確保員工安全與業務即時回復正常作業。

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. 名詞定義

無。

4. 權責

無。

5. 要求事項

5.1 學術網路服務（對外）障礙偵測與復原

當網路出現對外（Internet）連線問題，應先通知電算中心網路管理人員，並依下列程序執行障礙偵測與復原：

5.1.1 確認對外網路是否暢通

(1)檢查方法：網路管理人員以連往外部網站（例如入口網站）之測試方式來確認對外網路是否暢通。

(2)檢查結果：網站若無回應，請繼續以下步驟。

5.1.2 檢查網路回應狀態

(1)檢查方法：網路管理人員執行“tracert”網路指令來檢查網路回應狀態。（指令範例：tracert tw.yahoo.com）

(2)檢查結果：校外路徑無回應，填寫「資訊安全事件報告單」與執行資通安全通報應變作業程序流程。若校內無回應繼續以下步驟。

5.1.3 確認障礙原因是否為內部網路故障

(1)檢查方法：網路管理人員執行“ping”網路指令來檢查閘道器（Gateway）是否運作。（指令範例：ping 168.95.1.1）

(2)檢查結果：

結果一：若有回應，繼續 5.1.4 步驟。

結果二：若沒有回應，則初步判斷應為內部網路故障，請依「校園網路障礙偵測與復原」程序進行處理。

5.1.4 檢查相關網路安全設備與網路通訊設備是否正常運作

5.1.4.1.防火牆設備檢查

(1)檢查方法：網路管理人員檢查防火牆設備燈號是否顯示正常運作。

(2)檢查結果：

結果一：設備正常運作，繼續以下步驟。

結果二：若燈號顯示不正常，則初步判斷應為硬體故障，請進行設備更換或維修（依據「外部單位聯絡清單」聯絡相關廠商或單位協助處理）。

5.1.4.2.IPS、IDS 設備檢查

(1)檢查方法：網路管理人員檢查 IPS、IDS 設備是否正常運作及相關組態設定是否正確。

(2)檢查結果：

結果一：設備正常運作，繼續以下步驟。

結果二：若燈號顯示不正常，則初步判斷應為硬體故障，請進行設備更換或維修（依據「外部單位聯絡清單」聯絡相關廠商或單位協助處理）。

5.1.4.3.骨幹交換器（Switch）檢查

(1)檢查方法：網路管理人員檢查骨幹交換器（Switch）設備燈號是否顯示正常運作。

(2)檢查結果：

結果一：設備正常運作，繼續以下步驟。

結果二：若燈號顯示不正常，則初步判斷應為硬體故障， 請進行設備更換或維修（依據「外部單位聯絡清單」聯絡相關廠商或單位協助處理）。

5.1.4.4.校內交換器（Switch）檢查

(1)檢查方法：網路管理人員檢查交換器（Switch）設備燈號是否顯示正常運作。

(2)檢查結果：

結果一：設備正常運作，繼續以下步驟。

結果二：若燈號顯示不正常，則初步判斷應為硬體故障，請進行設備更換或維修（依據「外部單位聯絡清單」聯絡相關廠商或單位協助處理）。

5.1.5 執行實體線路檢查

如發現障礙原因為線路問題，則需按照線路叫修程序請相關電信服務廠商進行處理。

5.1.5.1.檢查方法：網路管理人員檢查骨幹交換器與區網中心間線路是否正常。

5.1.5.2.檢查結果：

結果一：若相關燈號顯示區網中心是正常運作，請依「校園網路障礙偵測與復原」程序進行處理。

結果二：若相關燈號顯示區網中心不是正常運作，則初步判斷

應為連外實體線路故障，通知相關電信服務廠商進行線路修復，並於修復完成時重新執行實體線路檢查步驟。

5.1.6 進行網路系統服務中斷事件處理檢討

5.1.6.1.復原狀況檢討：向資訊安全推動小組召集人報告處理進度與狀況。

5.1.6.2.事件處理檢討：針對「學術網路服務（對外）障礙偵測與復原」處理程序中有窒礙難行或可改進的步驟來進行討論與回饋。

5.2 校園網路服務障礙偵測與復原

當校園網路（Intranet）連線出現異常，應先通知電算中心網路管理人員，依下列程序執行障礙偵測與復原：

5.2.1 偵測網路設備運作

(1)檢查方法：網路管理人員利用網路管理軟體偵測電算中心網路設備是否正常運作。

(2)檢查結果：若有異常狀況，填寫「資訊安全事件報告單」與執行資通安全通報應變作業程序流程，並繼續以下步驟。

5.2.2 檢查網路設備狀態

(1)檢查方法：網路管理人員檢查有異常狀況之網路設備的狀態燈號。

(2)檢查結果：

結果一：若燈號顯示狀態正常，則表示網路設備間線路可能有異常，則檢查網路線路故障位置，並予以修復。修復後重新偵測電算中心網路設備是否正常運作。

結果二：若燈號顯示狀態異常，則聯絡設備維護廠商進行設備修復或更換（依據「外部單位聯絡清單」），並於修復期間以替代設備維持網路運作。

5.2.3 通報處理狀況與檢討

進行網路系統服務中斷事件處理檢討。

(1)復原狀況檢討：向資訊安全推動小組召集人報告處理進度與狀況。

(2)事件處理檢討：依據「校園網路障礙偵測與復原」處理程序中有窒礙難行或可改進的步驟進行討論與回饋。

5.3 校務系統障礙偵測與復原

當校務系統出現異常時，應先通知電算中心校務系統負責人員，依下列程序執行障礙偵測與復原：

5.3.1 偵測校務系統運作

5.3.1.1.系統管理人員檢查內部網路之通阻情形。
5.3.1.2.系統管理人員檢查系統主機設備是否運作正常。
5.3.1.3.執行校務系統主機設備、磁碟陣列等是否正常運作檢查。
5.3.1.4.執行校務系統資料庫存取檢查。
5.3.1.5.執行校務系統錯誤訊息檢查。

5.3.2 事件通報：若檢查有異常狀況，填寫「資訊安全事件報告單」與執行資通安全通報應變作業程序，並繼續以下步驟。

5.3.3 進行校務系統服務中斷事件處理檢討。

5.3.4 復原程序：

5.3.4.1.如發現障礙原因為設備故障，依設備維修流程進行處理。
5.3.4.2.如發現障礙原因為網路障礙，通知網路管理人員協助處理與復原。
5.3.4.3.如發現障礙原因為軟體服務運作問題，進行軟體設定檢查與復原，回復上一次運作正常之設定。必要時以備份資料回復伺服器。

5.4 電子郵件服務障礙偵測與復原

當電子郵件服務出現異常時，應先通知電算中心電子郵件管理人員，依下列程序執行障礙偵測與復原：

5.4.1 偵測電子郵件服務運作

5.4.1.1.網路管理人員檢查連外與內部網路之通阻情形。
5.4.1.2.網路管理人員檢查電子郵件主機設備是否運作正常。
(1)執行 SMTP 伺服器運作檢查。
(2)執行 POP3 伺服器運作檢查。
(3)執行垃圾郵件閘道運作檢查。
(4)執行 DNS 伺服器運作檢查。
(5)執行電子郵件主機錯誤訊息檢查。

5.4.2 事件通報：若檢查有異常狀況，填寫「資訊安全事件報告單」與執行 資通安全通報應變作業程序流程，並繼續以下步驟。

5.4.3 進行電子郵件服務中斷事件處理檢討。

5.4.4 復原程序：

5.4.4.1.如發現障礙原因為設備故障，依設備維修流程進行處理。
5.4.4.2.如發現障礙原因為網路障礙，通知網路管理人員協助處理與復原。
5.4.4.3.如發現障礙原因為軟體服務運作問題，進行軟體設定檢查與復原，回復上一次運作正常之設定。必要時以備份資料回復伺服器。

5.5 校園網頁服務障礙偵測與復原

當校園網頁服務出現異常時，應先通知電算中心校園網頁管理員，依下列程序執行障礙偵測與復原：

5.5.1 偵測校園網頁服務運作

5.5.1.1.系統管理人員檢查內部網路之通阻情形。

5.5.1.2.系統管理人員檢查系統主機設備是否運作正常。

5.5.1.3.執行校園網頁服務主機設備、磁碟陣列等是否正常運作檢查。

5.5.1.4.執行校園網頁服務資料庫存取檢查。

5.5.1.5.執行校園網頁服務錯誤訊息檢查。

5.5.2 事件通報：若檢查有異常狀況，填寫「資訊安全事件報告單」與執行 資通安全通報應變作業程序流程，並繼續以下步驟。

5.5.3 進行校園網頁服務中斷事件處理檢討。

5.5.4 復原程序：

5.5.4.1.如發現障礙原因為設備故障，依設備維修流程進行處理。

5.5.4.2.如發現障礙原因為網路障礙，通知電算中心網路管理人員協助處理與復原。

5.5.4.3.如發現障礙原因為軟體服務運作問題，進行軟體設定檢查與復原，回復上一次運作正常之設定。必要時以備份資料回復伺服器。

5.6 短時間內無法立即解決問題時

5.6.1 若半小時內找不到原因或問題無法解決或關機重開無法解決，發出通知並公告。

5.6.1.1 若有配備負載平衡，則立即啟動負載平衡運作。

5.6.1.2 若有配備備援系統，則立即啟動備援系統上線。

5.6.1.3 若以上功能都沒有配備或失效，則應立即建立新系統。

5.6.2 若 2 小時內備援系統無法上線或系統重新安裝還是無效。

5.6.2.1 系統設備關機斷網進行維護。

5.6.2.2 設定新設備處置時間最長 4~8 小時，系統重置上線。

6. 相關文件

6.1 資訊安全事件報告單。

6.2 外部單位聯絡清單。

6.3 臺灣學術網路各級學校資通安全通報應變作業程序。