

國立臺南第一高級中學

關鍵業務障礙偵測與復原作業程序

機密等級：敏感

文件編號：TNFSH-ISMS-C-003

版 次：1.0

發行日期：108.11.20

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

目錄

1	學術網路服務（對外）障礙偵測與復原	1
2	校園網路服務障礙偵測與復原	3
3	校務系統障礙偵測與復原	5
4	相關文件	8

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

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，應先通知本校網路管理人員，並依下列程序執行障礙偵測與復原：

1.1 確認對外網路是否暢通

1.1.1 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。

1.1.2 檢查結果：網站若無回應，請繼續以下步驟。

1.2 檢查網路回應狀態

1.2.1 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）

1.2.2 檢查結果：無回應，填寫「資訊安全事件報告單」與執行安全事件通報與應變作業流程。繼續以下步驟。

1.3 確認障礙原因是否為內部網路故障

1.3.1 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 X.X.X.X）

1.3.2 檢查結果：

結果一：若有回應，繼續 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。

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

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

1.4.1 防火牆設備檢查

1.4.1.1 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。

1.4.1.2 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)。

1.4.2 交換器 (Switch) 檢查

1.4.2.1 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。

1.4.2.2 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)。

1.4.3 路由器 (Router) 檢查

1.4.3.1 檢查方法：網路管理人員檢查路由器 (Router) 設備燈號是否顯示正常運作。

1.4.3.2 檢查結果：

結果一：設備正常運作，繼續以下步驟。

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

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）。

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。

1.5.1 檢查方法：網路管理人員檢查線路是否正常。

1.5.1.1 檢查結果：

結果一：若相關燈號顯示正常運作，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步驟 1.4 再進行確認。

1.6 進行網路系統服務中斷事件處理檢討

1.6.1 復原狀況檢討：向資訊安全官報告處理進度與狀況。

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。

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，應先通知本校網路管理人員，依下列程序執行障礙偵測與復原：

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

2.1 偵測網路設備運作

2.1.1 檢查方法：網路管理人員利用網路管理軟體偵測本校網路設備是否正常運作。

2.1.2 檢查結果：若有異常狀況，填寫「資訊安全事件報告單」與執行安全事件通報與應變作業流程，並繼續以下步驟。

2.2 檢查網路設備狀態

2.2.1 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。

2.2.2 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。修復後重新偵測本校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。

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。

2.3.1 復原狀況檢討：向資訊安全官報告處理進度與狀況。

2.3.2 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。

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

3 校務系統障礙偵測與復原

當校務系統出現異常時，應先通知本校系統負責人員，依下列程序執行障礙偵測與復原：

3.1 偵測校務系統運作

3.1.1 系統管理人員檢查系統主機設備是否運作正常。

3.1.1.1 檢查步驟：至校務系統資料庫主機 X.X.X.X 察看主機電源是否正常，機體是否不正常發熱，有無不正常聲響或警示聲音發生。

3.1.2 執行校務系統主機設備、磁碟陣列等是否正常運作檢查。

3.1.2.1 檢查步驟：至校務系統資料庫主機 X.X.X.X 察看主機磁碟陣列是否正常運行，並至 BIOS 查看磁碟陣列的使用狀態是否 online，再者能否正常登入作業系統，並查看系統事件日誌是否有異常紀錄。

3.1.3 系統管理人員檢查內部網路之通阻情形。

3.1.3.1 檢查步驟一：至校務系統資料庫主機 X.X.X.X 察看網路卡燈號是否正常閃爍，若無正常閃爍請檢查網路卡接頭及所連接網路線是否異常。

3.1.3.2 檢查步驟二：登入作業系統，在命令提示字元下輸入「ping 127.0.0.1」測試網路卡驅動程式是否已安裝。

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

3.1.3.3 檢查步驟三：接著輸入「ping X.X.X.X」測試網路卡硬體是否正常，若無回應察看網路連線設定是否正常，若正常且利用別台主機下 arp 可取得此台 mac 位址，則可判斷網路卡驅動程式異常，重新安裝網路卡驅動程式。

3.1.3.4 檢查步驟四：接著再測試「ping www.hinet.net」判斷 DNS 以及對外連線是否正常，若皆正常，查看網路連線防火牆的設定是否阻擋連線。

3.1.3.5 檢查步驟五：若以上正常，則執行 ping 相關指令，檢查使用者端 IP 是否正常連線。

3.1.4 執行校務系統資料庫存取檢查。

3.1.4.1 檢查步驟一：至校務系統資料庫主機 X.X.X.X，利用資料庫管理工具執行資料庫連線，查看資料庫的服務是否執行中，並點選「管理」/「目前活動」，檢查是否有使用者資料庫連線被鎖定造成其他使用者無法連接。

3.1.4.2 檢查步驟二：至系統管理工具/事件檢視器，檢查是否有資料庫連接錯誤訊息紀錄。

3.1.5 執行校務系統錯誤訊息檢查。

3.1.5.1 檢查步驟一：至校務系統資料庫主機 X.X.X.X，檢查

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

除 Windows 預設防火牆之外，另有安裝免費防火牆軟體，開啟此防火牆軟體檢查是否阻擋校務系統使用者 IP 的連接，或防火牆異常造成連接錯誤。

3.1.5.2 檢查步驟二：若主機正常，請至使用者端查看使用者登入錯誤狀況為何，以判斷是否為軟體更新安裝後導致連接錯誤。

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」與執行安全事件通報與應變作業流程，並繼續以下步驟。

3.3 進行校務系統服務中斷事件處理檢討。

3.4 復原程序：

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，若為資料庫主機故障且處理時間需超過 24 小時，視情況將資料庫備份資料回復至其他備用主機伺服器，更改主機 IP 或校務系統存取位址，以利系統持續運作。

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。

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主機。

關鍵業務障礙偵測與復原作業程序

文件編號	TNFSH-ISMS-C-003	version	1.0	機密等級	敏感
------	------------------	---------	-----	------	----

4 相關文件

4.1 資訊安全事件報告單

4.2 外部單位聯絡清單