淡江大學資訊中心 IDC 機房
資訊安全事件處理辦法

編號：FIHX-ISMS-02010

版本 1.6

簽核欄	
審核	
覆核	
本辦法經主任覆核後實施，修正時亦同。	

機密等級：一般資訊	文件負責人：蔡春枝
修訂日期：98.01.12	公告日期：98.02.24

版本變更紀錄：

變更日期	文件版本	編訂者	變更紀要說明
93.5.13	1.1	張慧君	依資訊安全管理系統文件及紀錄管理辦法中文件層級要求將第二層級之文件統一改為辦法。 (資訊安全事件處理規則改為資訊安全事件處理辦法)
93.6.23	1.2	張慧君	依內部稽核結果經委員會覆核後修訂
93.11.05	1.3	蔡春枝	1.文件負責人由張慧君改為蔡春枝 2.附件二：相關人員聯絡單異動：張慧君改為蔡春枝；馮心萍改為張碧君；劉佳欣移除；TSM 資料備份、回復：姜美文、張淑美改為姜美文、郭嘉萍；儲域網路系統：新增郭嘉萍
94.08.10	1.4	張碧君	附件二：相關人員聯絡單異動 網路安全人員、儲域網路系統成員列入張佑嘉
95.03.27	1.5	蔡春枝	修訂： 1.肆、第三項(一)~(五) 2.伍、第一項增修第(二)條 2.及第二項(五)1. 3.增修 陸、參考文件 4.修訂 捌、附件二相關人員聯絡單為權責相關人員編制及聯絡電話表，列入參考文件 5.增修附件一及附件三內容,附件三改為附件二 6.增修附表一
98.01.12	1.6	蔡春枝	重審修訂

目　　錄

壹、目標

為防範IDC機房實體維運及TSM資料備份、回復作業相關系統造成損害或不當使用等資訊安全事件、事故發生而影響營運，並能迅速依緊急通報程序向相關人員反應通報，以加強處理的效率及時程掌控，降低事件、事故可能帶來之損害。

貳、適用範圍

無論來自於人為故意或不經意的，或不可抗力的因素，任何導致IDC機房實體維運、TSM資料備份、回復及備份機房電腦系統非正常運作的情況均適用之。

參、權責

一、 資訊安全事件、事故發生時，利用資訊安全事件通報機制向機房值班人員、資訊安全作業小組或資訊安全官，進行資訊安全事件通報作業。

二、 資訊安全作業小組依據所通報之資訊安全事件內容進行分析暨初步處理。

肆、控制要點

一、 資訊安全事件通報及受理程序說明。

二、 資訊安全事件分析及處理程序說明。

三、 名詞定義：

(一)事件：任何發生在系統或網路、或進出監控系統，機房值班人員可觀察到之變化。

(二)資訊安全事件：資訊安全事件是系統、服務或網路顯示可能危害資訊安全政策或安全保證失效的狀態，或是可能與安全相關、先前未知的狀況等的一次識別的發生。

(三)資訊安全事故：資訊安全事故是有重大可能危及營運作業與威脅資訊安全的單一或一連串有害的或意外的資訊安全事件。

(四)由於本 ISMS 系統對於資訊安全事件與事故已依影響程度合併分級處理，以下皆以資訊安全事件代表說明。事件等級說明詳(附表一)

(五)系統或設備異常：系統或設備出現不正常之狀況，由系統或設備負責人記錄、分析及處理。

伍、要求事項

一、 資訊安全事件通報及受理程序

(一) 資訊安全事件通報作業人員編組架構

資訊安全事件通報受理人員

1.資訊安全作業小組

2.資訊安全官

3.機房值班人員

4.資訊安全事件通報作業受理人員編制(附件一)

(二) 資訊安全事件通報流程

1.資訊安全事件發生時，由發現人/使用者(End User)利用通報機制向資訊安全作業小組相關人員通報事件內容(非正常上班時間則向機房值班人員通報，再視情況轉報資訊安全作業小組相關人員)。

2. 資訊安全作業小組相關人員接受到通知後判斷事件性質、等級及預估事件處理時間，並立即反應給資訊安全官，然後填寫「資訊安全事件通報/處理紀錄表」，將事件登錄及編號。

3. 由資訊安全官進行初步決策及協調溝通作業。

4. 當資訊安全事件等級較低、威脅性較小時(為 A 級以下事件時)，可由資訊安全官進行必要之決策，詳細作業流程參閱(附圖一)。

5. A 級之資訊安全事件，由「資訊安全委員會」進行對外(主管機關)通報作業。

6. 有關資訊安全事件等級詳(附表一)、資訊安全通報流程詳(附圖一)。

二、 資訊安全事件分析及處理程序

當資訊安全作業小組相關人員收到資訊安全事件之通報時，可依以下五大執行步驟及各作業流程，進行狀況分析及處理，處理方法可參考「資訊安全事件處理方法」 (附件二)。

(一)資訊安全事件辨識

由業務負責人判斷系統或設備運作不正常原因(例如下列原因)，並通知資訊安全官，如果可以應盡力記錄相關訊息和蒐集證據，以備事後查驗。

1. 服務、設備或設施的損失
2. 系統異常、故障或超載
3. 軟體或硬體的故障
4. 人為錯誤
5. 未遵循政策或指引
6. 違反實體的安全協議
7. 未加以控制的系統變更

8. 違反存取的規範
9. 駭客入侵或網路攻擊事件
10. 或其他災害

(二) 資訊安全事件抑制

針對異常狀況，須進行記錄並由業務負責人判定是否為設備或系統產生狀況，再依各種狀況採取緊急抑制方法。

(三) 資訊安全事件移除

1. 瞭解資訊安全事件之原因。
2. 移除資訊安全事件成因：設備不良、人為破壞、駭客入侵、新系統上線、新設施加入...等。

(四) 復原階段

1. 回復作業狀態。
2. 持續監視作業運作，確認系統屬於正常狀態。

(五) 追踪階段：相關執行內容如下：

1. 由資訊安全官負責覆核事件報告，並呈報「資訊安全委員會」討論是否修訂「資訊安全管理系統政策」或相關安全辦法與規則。
2. 重新進行資產清查，並檢視是否有類似作業遭受波及。
3. 保存所有事件移除分析、處理紀錄，並與相關單位或人員進行事後檢討，視需要進入矯正預防措施，參照「矯正預防措施管理辦法」。應評估未來再發生或造成重大衝擊事故之可能，以確認是否應加強控制措施。

陸、參考文件

一、 業務持續運作管理辦法

二、 資訊安全組織辦法

三、 矯正預防措施管理辦法

四、 權責相關人員編制及聯絡電話表

柒、相關表單

一、資訊安全事件通報/紀錄表

捌、附件

附件一：資訊安全事件通報作業受理人員編制。

附件二：資訊安全事件處理方法。

附表一：資訊安全事件影響嚴重程度分級。

附圖一：資訊安全事件通報流程。

附件一：資訊安全事件通報作業受理人員編制

一、基本編組

小組名稱	資訊安全事件通報受理成員
資訊安全事件受理人員編組	資訊安全作業小組 (包含電腦防毒人員、網路安全人員、實體環境安全人員、系統安全人員、資訊安全專員)
	資訊安全官
	機房值班人員

二、人員工作職掌

資訊安全事件受理人員編組

(一) 資訊安全作業小組成員：電腦防毒人員、網路安全人員、實體環境安全人員、系統安全人員、資訊安全專員(詳資訊安全組織辦法)。

主要職掌：

1.確定事件本質 (排除誤報狀況)。

2.識別事件種類 (性質)。

3.決定事件等級及預估事件所需處理時間。

4.執行相關人員通報作業。

5.設法排除資訊安全事件，回復正常作業。

6.撰寫事件處理相關報告或表單。

7.配合執行教育訓練工作。

(二) 資訊安全官

主要職掌：

1.針對事件性質類別及等級等因素提出解決方案之建議。

2.與資訊安全小組及支援單位保持溝通，並協調必要支援作業。

3.當事件威脅性較低時，代表「資訊安全委員會」執行通報作業決策。

4.協助資訊安全委員會處理相關事宜。

5.依據「資訊安全委員會」指示執行事件處理作業。

6.蒐集並保全事件相關資訊及執行成果。

7.擬訂及執行教育訓練計畫。

(三) 機房值班人員

主要職掌：

1.非正常上班時間當資訊安全事件發生時，則由機房值班人員針對安全事件性質通知消防、警衛、作業系統負責人及資訊安全官等進行事件處理。

2.依作業負責人員或資訊安全官指示，辦理事件處理工作。

附件二：資訊安全事件處理方法

一、資訊安全事件辨識

(一) 狀況分析

1. 網路中斷

(1)檢查、確認網路連線

自其他機器 PING 設備 IP 位置

->斷線確認，通知網路管理組處理。

2. 服務中斷

(1)於本機嘗試登入提供服務之系統，是否可正常登入，若否，則確認系統已遭受入侵或攻擊。

->確認遭受入侵或攻擊，進行入侵證據取得階段。

(2)檢查服務選項是否顯示服務中，若否，則嘗試再次正常啟動之。

->確認遭受入侵或攻擊，進行入侵證據取得階段。

(3)系統是否出現不正常之警告訊息。若否，則檢視系統稽核紀錄，含服務稽核紀錄與作業系統之稽核紀錄，檢視是否存在異常狀況紀錄並至原廠網站取得錯誤訊息檔案或參考操作管理手冊確認各訊息代表意義。

(4)如稽核紀錄檔案為空白(系統於先前已啟動相關稽核功能)，則確認遭受入侵或攻擊，進行入侵證據取得階段。

(5)若已成功取得所有稽核紀錄並匯出保管後，則嘗試重新開機。若重新開機後，無法登入系統，則確認遭受入侵或攻擊，進行抑制階段作業。

3. 通訊異常

(1)透過指令(netstat -na，UNIX 與 NT 環境均適用)、或使用通訊埠掃描器執行待確認主機之通訊埠掃描，確認是否開啟異常通訊服務埠，並至 IANA 網站查詢。

http://www.iana.org/assignments/port-numbers

(2)透過指令(netstat -na，UNIX 與 NT 環境均適用)、確認是否存在異常連線來源 IP 位置。判定來源 IP 位置，是否合理，否則請網路管理組處理。

(3)檢視系統之服務(SERVICE)、背景程式(DAEMON、PROCESS)，檢視是否存在異常服務名稱。

4. 中毒與攻擊

使用掃毒軟體，檢測主機是否存在病毒檔案(包含木馬、後門與惡意程式等)，倘若發現中毒訊息，則判定為人為惡意上傳或系統漏洞導致。

(二) 證據取得與保留

1. 存取作業系統之稽核功能所留下之稽核紀錄檔案，並將各檔案匯出保管。
2. 透過列印畫面方式，留下異常訊息畫面。
   (1) 通報各相關部門：依計劃設定方式通報可能被影響之部門。
   (2) 與維護廠商保持合作。

二、 資訊安全事件抑制

由作業系統負責人依據各狀況採取下列緊急抑制方法。

(一) 若為木馬、後門程式，則立即刪除或移除該木馬與後門或背景程式(DAEMON OR PROCESS)。若為病毒，則立即進行中斷網路連線之程序。

(二) 中斷連線

1. 視系統之重要程度，及時公告停止服務訊息後，立即終止網路連線，將網路線拔除。
2. 請網路管理組，針對異常主機 IP 位置，進行通訊封鎖。

(三) 存取權限限制

1. 透過稽核紀錄檢視該事件是否有存取相關電腦資料，並立即調整該資料之相關存取權限。
2. 透過稽核紀錄檢視資安事件所使用之帳號資訊，並立即停止使用該帳號與變更密碼。

(四) 獨立出發生問題之系統、環境。

三、 資訊安全事件移除

(一) 瞭解資訊安全事件之攻擊方式。

(二) 移除資訊安全事件成因：例如設備不良、人為破壞、駭客入侵、新系統上線、新設施加入。

(三) 執行方式：

1. 透過防毒程式進行系統掃描，針對已中毒檔案，需視嚴重程度適度給予病毒移除與檔案還原，對於無法回覆之檔案應考量刪除該檔案，或僅將重要資料檔案備份後進行系統重建作業。
2. 對於不需使用之服務應予以停用，並透過系統功能限制相關通訊埠之連接存取。
3. 針對存在漏洞之服務，應立即進行修補，並依據各狀況，移除相關木馬、後門與惡意程式。倘若未能移除該惡意程式碼時，應將重要資料備份後，進行系統重建。
4. 移除之技術需與委外廠商研討因應對策與移除之可能性。
5. 為避免系統重要資訊流失與遭竊，對於遭受入侵與被安裝木馬、後門隻惡意

之主機，應以系統重建為第一優先之考量，唯進行重建前，應先將重要要資料備份並進行還原測試後始可進行。

四、復原階段

由系統負責人處理，並通知「資訊安全官」—相關執行內容如下：

(一) 回復系統狀態

1. 系統還原後，應立即安裝修正程式，於修正程式安裝前不應連接網路。
2. 系統還原後，應檢視其通訊狀況(NETSTAT)，並檢視其相關服務(UNIX 系統之 PS –AXU OR NT 系統之服務檢視)，如發現不明服務應停止連接網路。
3. 無論系統還原，或新系統安裝，各系統均應完成適當權限設定，移除不需要之服務、帳號、目錄、檔案與存取權限。

(二) 持續監視系統運作，確認系統屬於正常狀態。

五、追踪階段

相關執行步驟如下：

(一) 重新進行資產清查，並檢視是否有類似系統遭受波及。

(二) 保存所有事件移除、分析、處理紀錄，並與相關單位或人員進行事後檢討會議。

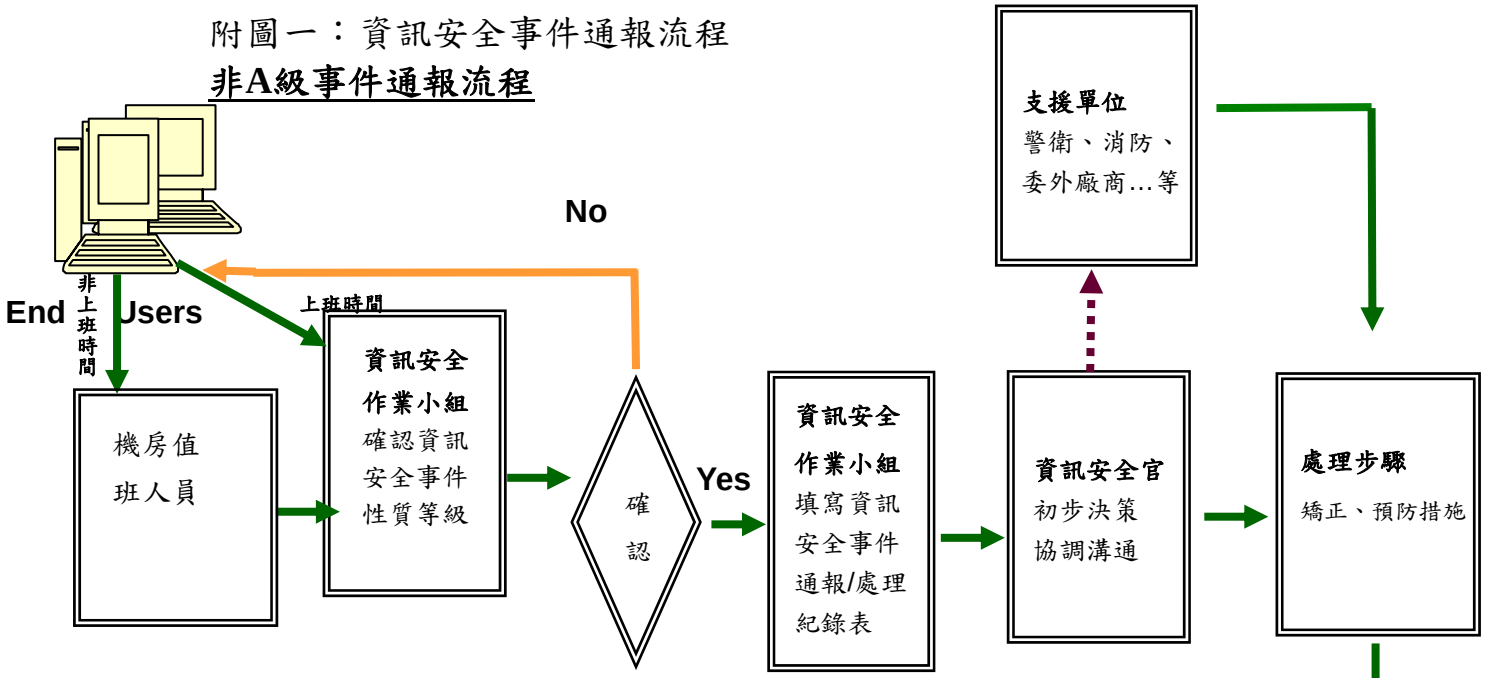
(三) 資訊安全官應定期將事件，提報「資訊安全委員會」討論是否修訂「資訊安全政策」或相關安全辦法與規則，並執行「資訊安全委員會」指示之改善動作，視需要進行教育訓練以防止再次的資訊安全事件發生。

附表一：資訊安全事件影響嚴重程度分級

等級名稱	資訊安全事件影響程度說明
A	服務中斷，需一天以上始可修復，嚴重影響中心營運
B	服務嚴重停頓，一天內可修復
C	服務短暫中斷；判斷監控到實體或網路環境未授權之存取影響層面嚴重
D	服務延遲，可立即處理恢復效率或監控到實體或網路環境未授權之存取
E	不影響服務，但持續發生可能影響服務之提供。

附圖一：資訊安全事件通報流程

非A級事件通報流程



A級以上事件通報流程