環球科技大學

文件名稱	資安事件通報及危機處理管理程序	版本	4.0
文件編號	ISMS-02-011	發行日期	2016/10/07
		頁次	1 / 6

1.目的：

1.1 規範圖書資訊處實施永續營運管理作業，結合強化和矯正復原控制措施，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 明確規範資訊或個資安全事件通報與事故處理相關作業規定及作業權責。

1.3 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：

圖書資訊處網路骨幹管理與所提供之機房維運服務及校務資訊系統服務與維運作業。

3.權責：

3.1 執行秘書：

3.1.1 覆核重要系統災害復原及復原後之測試結果。

3.1.2 覆核資訊或個資安全矯正措施報告資料。

3.1.3 負責圖書資訊處資訊或個資安全事件通報與事故處理應變作業成敗之責。

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 判定資訊或個資安全徵兆，協助鑑別資訊或個資安全事件。

3.2.7 負責系統紀錄與稽核軌跡等證據保全工作。

3.3 資訊安全組：

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。

4.名詞解釋：

4.1 資訊或個資安全事件：系統、服務或網路發生一個已識別的狀態，其指示可能的資訊或個資安全政策違例或防護措施失效，或可能與資訊或個資安全相關而先前未知的狀況等。例如：網路流量大增、連線速度緩慢，且由防火牆日誌中發現有異常之連線紀錄，但尚未導致資訊系統主要功能降低或喪失。

4.2 資訊或個資安全事故：單一或一連串非預期的資訊或個資安全事件，有可能構成資訊或個資安全事故。如果該等資訊或個資安全事件已使機密洩露或影響業務主要運作，或顯著可能造成圖書資訊處資訊資產機密性、完整性及可用性遭破壞時，即構成資訊或個資安全事故。例如：經由分析研判，確認駭客針對 Web 伺服器傳送大量特定封包，因而導致網站癱瘓，資訊系統主要功能之部份降低或喪失。

5.作業內容：

5.1 日常監控作業

圖書資訊處資訊作業環境應建立安全監控機制，以偵測違反資訊安全規範之行為，並記錄所監控之事件，以便發生資訊或個資安全事故時，提供佐證之用；安全監控機制應包含下事項：

5.1.1 資產使用及數量監控。

5.1.2 實體環境安全監控。

5.1.3 網路存取監控。

5.1.4 應用系統存取監控。

5.1.5 作業系統存取監控。

5.1.6 資料庫存取監控。

5.1.7 機房操作人員作業監控。

5.2 事件通報作業

5.2.1 為建全通報體系，應建立並維護包含校內同仁與相關服務廠商之「資訊安全組織成員表」與「廠商聯絡清單」。

5.2.2 圖書資訊處內部資訊安全事件危機通報作業程序如下：

5.2.2.1 圖書資訊處同仁如發現資訊或個資安全事件時，發現同仁應填寫「資訊安全事件通報單」通報人資料、通報內容、勾選事件影響等級與破壞程度，並立即(最遲不得超 1 小時)向資訊安全組反應。

5.2.2.1.1 事件影響等級說明：(教育機構資安通報應變手冊所使用之事件等級)

4 級

(1).國家機密資料遭洩漏。

(2).國家重要資訊基礎建設系統或資料遭竄改。

(3).國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

3 級

(1).密級或敏感公務資料遭洩漏。

(2).核心業務系統或資料遭嚴重竄改。

(3).核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

2 級

(1).非屬密級或敏感之核心業務資料遭洩漏。

(2).核心業務系統或資料遭輕微竄改。

(3).核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

1 級

(1).非核心業務資料遭洩漏。

(2).非核心業務系統或資料遭竄改。

(3).非核心業務運作遭影響或短暫停頓。

0 級 –違反電腦網路使用規範。（不須通報教育機構資安通報平台）

5.2.2.2 資訊安全組接獲「資訊安全事件通報單」通知後，判斷事件相關之設備(系統)，聯絡系統(主機)管理員或負責人員共同判別是否為資訊或個資安全事件。

5.2.2.3 事件處理：

5.2.2.3.1 經事件判定，不會影響到本校正常運作，由資訊安全組在「資訊安全事件通報單」事件是否成立欄位上勾選「否」，由資訊安全組說明勾選原因，再請資訊安全組將通報單留存。

5.2.2.3.2 若事件類別為 0 級、1 級與 2 級，且尚未導致資訊系統主要功能降低或喪失之資訊或個資安全事件，資訊安全組應在「資訊安全事件通報單」事件是否成立欄位上勾選「是」，再請事件負責人填寫通報單之欄位，欄位名稱為”資訊安全事件來源（原因）說明與分析”，並依「資訊安全矯正管理程序」開立「矯正措施處理單」或填寫「資訊安全事件/事故處理單」進行資安事件的矯正。

5.2.2.3.3 如果事件類別為 3 級與 4 級，又經過資訊安全組與聯絡系統(主機)管理員或負責人員共同判別為資訊或個資安全事件，且造成資訊系統主要功能部份降低或喪失時，即成為『資訊或個資安全事故』，屆時事故負責人員依「資訊安全事件通報單」填寫「資訊安全事件/事故處理單」，並且通報執行秘書，透過資訊安全組成立緊急處理組進行事故處理。

5.2.2.4 依教育機構資安通報應變手冊之規定，事件類別為 1 級、2 級、3 級與 4 級，圖書資訊處資安聯絡人應依規定到教育機構資安通報平台上填寫通報內容。

5.2.2.5 資訊或個資安全事件造成同仁生命安全或設備遭到破壞等涉及民事或刑事案件時，應通報檢調單位請求支援並協助處理。

5.3 事故辨識作業

5.3.1 經資訊安全組與聯絡系統(主機)管理員或負責人員共同判別事件類別為3級與4級為資訊或個資安全事故後，事故負責人員應依「資訊安全事件/事故處理單」進行事故處理。

5.3.2 事故負責人員應依資訊或個資安全事故狀況協調設備(系統)管理人員辦理事故辨識作業，並將辨識結果紀錄在「資訊安全事件/事故處理單」之資安事故辨識作業欄位中。

5.3.3 辨識工作完成前，應儘可能避免系統重新開機，以保全完整證據，若系統必須重新開機，則應於重新開機前保留系統稽核紀錄檔案。

5.4 事故抑制作業

5.4.1 處理事故單位負責人應依資訊或個資安全事故辨識結果，針對異常狀況協調系統(主機)管理員採取緊急抑制措施，並將抑制方法與注意事項紀錄在「資訊安全事件/事故處理單」。

5.4.2 緊急抑制措施應以隔離或停止事故發生之設備、系統、環境及存取權限或連線為原則。

5.5 事故排除作業

5.5.1 處理事故單位負責人應依資訊或個資安全事故發生之原因，協調系統(主機)管理員進行事故排除作業。

5.5.2 為避免事故排除作業造成重要資料或鑑識證據之遺失，應於事故排除作業前完成重要設定檔、資料與鑑識紀錄檔之備份。

5.5.3 備份作業完成後，應確認備份資料之有效性與可用性，以避免備份失敗導致資料毀損。

5.5.4 事故排除作業除需移除資訊或個資安全事故原因外，應依事故發生原因加強防護，並將加強防護的措施紀錄在「資訊安全事件/事故處理單」作為往後資訊或個資安

全日常管理的參考，以避免相同事故再次發生。

5.6 系統復原作業

5.6.1 資訊或個資安全事故排除後，若有需要應由系統(主機)管理員或負責人員與資訊安全組進行系統復原作業。

5.6.2 系統(主機)管理員應於系統復原 3 天內，加強監視系統運作，確認系統屬於正常作業，並將每日監控的狀況紀錄於「資訊安全事件/事故處理單」。

5.7 事故檢討與學習

5.7.1 資訊或個資安全事故處理過程應由處理事故單位負責人填寫「資訊安全事件/事故處理單」，並保存所有事故移除分析及處理紀錄。

5.7.2 資訊或個資安全事故排除後，處理事故單位負責人與系統(主機)管理員進行事後檢討會議，擬定「災害復原演練規劃表」。

5.7.3 資訊安全事件/事故處理單，應提報「資訊安全管理委員會」討論是否修訂圖書資訊處相關安全政策與規範，以防止事故再次發生。

5.7.4 資訊或個資安全事故處理結果，在無牽涉個人隱私與圖書資訊處業務機密之情況，應定期彙整並公告於內部網站，描述事故發生原因、過程、處理方式、改善與注意事項等，做為內部資安宣導及事故防範之參考資訊。

6. 參考文件：

6.1 資訊安全矯正管理程序(ISMS-02-004)

7. 使用表單：

7.1 資訊安全組織成員表（ISMS-04-033）

7.2 廠商聯絡清單（ISMS-04-023）

7.3 資訊安全事件通報單(ISMS-04-034)

7.4 資訊安全事件/事故處理單(ISMS-04-035)

7.5 災害復原演練規劃表(ISMS-04-036)

7.6 矯正措施處理單(ISMS-04-006)