僑光科技大學
Overseas Chinese University

文件名稱：資安事件通報及危機處理管理程序 文件編號：OCU-2-008 制定單位：資訊中心 申請類別：□制定 ☑修訂 □廢止 機密等級：一般	文件發行章 僑光科技大學 資訊中心

NO	修訂日期	頁次	版本	修 訂 內 容 摘 要
1	2015.05.25	4	1	新制定
2	2016.02.15	3	2	修訂 1.目的：，3.權責：，5.2.2…及刪除表單 6.4、6.6
3.	2018.05.10	3	3	修訂 5.2.2.2.1、5.2.2.2、5.4.1…使用表單
4.	2022.09.29	4	4	依臺灣學術網路各級學校資通安全通報應變作業程序修訂，增加 4.3 資安等級、增修 5.2.2【註】、5.2.2.2.1 及調整 5.2.2.2.2、5.2.2.2.3

擬稿人	審查	核准
資訊中心 承辦 張群芳	資訊中心 承辦 賴麒祐	資訊中心 主任 林金成

僑光科技大學
Overseas Chinese University

1.目的：

1.1 明確規範資安事件通報與事故處理相關作業規定及作業權責。

1.2 有效掌握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：

有關資訊機房作業環境。

3.權責：

3.1 資訊安全工作小組：

3.1.2 覆核資訊安全矯正預防措施報告資料。

3.1.3 負責本組資安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 判定資安徵兆，協助鑑別資安事件。

3.2.2 負責系統紀錄與稽核軌跡等證據保全工作。

3.3 資訊安全稽核小組：

3.3.1 查核資訊安全矯正預防措施實施情形。

4.名詞解釋：

4.1 資訊安全事件：系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或防護措施失效，或可能與資訊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 資訊安全事故：單一或一連串非預期的資訊安全事件，有可能構成資訊安全事故。如果該等資訊安全事件已使機密洩露或影響業務主要運作，或顯著可能造成資訊資產機密性、完整性及可用性遭破壞時，即構成資訊安全事故。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。

4.3 資安事件等級：

4.3.1 4 級事件，符合下列任一情形者，屬 4 級事件：

1.一般公務機密、敏感資訊之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

2.一般公務機密、敏感資訊之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

3.核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

4.3.2 3 級事件，符合下列任一情形者，屬 3 級事件：

1.核心資通系統但未涉及關鍵基礎設備之一般公務機密、敏感資訊遭輕微洩漏。

2.涉及關鍵基礎設施之核心業務資訊或核心資通系統遭輕微竄改。

3.核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉

及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4.3.3 2 級事件，符合下列任一情形者，屬 2 級事件：

1.非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

2.非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

3.非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

4.3.4 1 級事件，符合下列任一情形者，屬 1 級事件：

1.非核心業務資訊遭輕微洩漏。

2.非核心業務資訊或非核心資通系統遭輕微竄改。

3.非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成日常作業影響。

4.3.5 資安預警事件，凡屬有待受害單位進行確認之資安事件皆屬於資安預警事件：

1.未確定事件或待確認事件單：來自北區教育學術資訊安全監控中心（N-ASOC）、南區教育學術資訊安全監控中心(S-ASOC)、縣市網資訊安全維運中心(MINI-SOC)使用之新型技術所產生之事件單，但正確性有待確認者。

2.其他單位所告知教育部所屬單位所發生未確定之資安事件。

5.作業內容：

5.1 日常監控作業

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「資安事件緊急聯絡單位」。

5.2.2 內部資訊安全事件危機通報作業程序如下：

如資安事件或事故來源為「教育機構資安通報平台」，依規定到該平台上填寫通報內容。其餘資訊安全事件相關通報處理程序依照下述辦理。

【註】如因網路或電力中斷等事由，致使無法上網填報資安事件，須於確認資安事件條件成立後 1 小時內，與所屬區網路中心及通報應變小組聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。

5.2.2.1 同仁如發現資訊安全事件時，發現同仁應填寫「資訊安全事件通報處理單」通報人資料、通報內容，並立即(最遲不得超 1 小時)向業務承辦人反應。

5.2.2.2 事件處理：

5.2.2.2.1「4」、「3」級資安事件須於 36 小時內完成損害控制或復原；「2」、「1」級資安事件須於 72 小時內完成損害控制或復原。

5.2.2.2.2 若事件影響等級為 1、2 級，資訊中心應依據「資訊安全矯正措施管理程序」，填寫「矯正措施處理單」。

5.2.2.2.3 若事件影響等級為 3、4 級則定義為事故，資訊中心除依據「資訊安全矯正措施管理程序」，填寫「矯正措施處理單」外，視需要依據「營運持續管理程序」執行營運持續。

5.2.2.3 資訊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

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「矯正措施處理單」。

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、資料與鑑識記錄檔之備份。

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「矯正措施處理單」作為往後資訊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內部稽核小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。

5.7 事故檢討與學習

5.7.1 資訊安全事故處理過程應由處理事故單位負責人填寫「矯正措施處理單」，並保存所有事故移除分析及處理紀錄。

5.7.2 資訊安全事故排除後，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 針對事件影響等級為 3、4 級，應提報「資訊安全委員會」討論是否修訂相關安全政策與規範，以防止事件再次發生。

5.7.4 資訊安全事故處理結果，在無牽涉個人隱私與業務機密之情況，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預防之參考資訊。

6.使用表單：

6.1 資訊安全組織成員表（OCU-4-002）

6.2 資安事件緊急聯絡單位（OCU-4-025）

6.3 資訊安全事件通報處理單（OCU-4-026）

6.4 災害復原演練規劃表（OCU-4-028）

6.5 矯正措施處理單（OCU-4-034）

7.相關文件：

資訊安全矯正措施管理程序（OCU-2-012）