三十五、人事室資安事件通報及處理標準作業流程

項目編號：SOP-A50-2-12-04　　制訂日期：098 年 09 月 30 日

業務單位：人事室　　修訂日期：100 年 06 月 17 日

業務項目	資安事件通報及處理作業
承辦人員	單心怡
聯絡電話	2232
e-mail	sis@cc.shu.edu.tw
作業時間	隨時
作業說明	1. 確保本校所管理之資訊資產免遭破壞或不當使用，以期能有效處理異常事件之預防、通報及危機處理等相關事宜，降低異常事件之影響，並能從異常事件的分析及檢討，發現資訊安全管理系統的改進機會。 2. 資安事件之預防須定期對學校有可能面臨的資安事件進行評估，如：透過風險評估方式，針對高風險之事件採取相關的預防措施。 3. 資安事件之分類 應依造成資安事件之原因、影響程度及範圍建立資安事件分類，確保事件發生時均能獲得適當的控制，以降低資安事件發生時所造成的影響。 (1) 重大/緊急事件 (造成服務中斷，且無法於目標回復時間內恢復之事件) ● 天然災害 (火災、地震、水災、颱風等) 造成服務中斷，且無法於目標回復時間內恢復。 ● 洩漏機密資訊或違反安全規定之故意行為或人為疏失，屬情節重大者。 ● 軟體失效 (資料庫、應用系統、作業系統)，且無法於目標回復時間內恢復。 ● 人事室教職員所使用的電腦全面中毒或遭駭客入侵。 ● 遭受病毒侵襲，且無法於目標回復時間內排除。 ● 其他造成服務中斷之重大事件。 (2) 一般安全事件 (造成服務中斷，但不致超過目標回復時間之事件) ● 洩漏一般資訊或違反安全規定之故意行為或人為疏失，屬情節輕微者。 ● 軟體失效 (資料庫、應用系統、作業系統)，但可於目標回復時間內恢復。 ● 駭客入侵，但未造成服務中斷。

	● 遭受病毒侵襲，但可於目標回復時間內排除。 (3) 其他安全事件 ● 無法歸類之其他事件。 ● 內部稽核發現缺失/外部稽核發現缺失。 ● 管理審查會議之缺失報告。
作業流程	一、資安事件之通報 1. 教職員之通報服務 ● 個人電腦異常:透過校內電話分機 2320 通報至電算中心服務台。 ● 人事系統或網路異常：通報電算中心系統組之負責窗口 (分機：2308、2317)。 ● 非人事系統異常：通報人事室之負責窗口 (分機：2238)。 2. 人事室服務信箱 由人事室對內提供的信箱，收到之事件通知。 3. 其它事件 由資訊安全稽核或其它會議討論發現之異常事件。 二、資安事件之紀錄內容 各事件之紀錄內容建議包含以下事項： ● 事件通報人員 ● 事件類別及通報管道 ● 事件通報時間 ● 事件內容描述 ● 事件登錄人員 ● 事件處理狀況 (是否已結案) ● 事件結案時間 三、事件應變處理 1. 教職員通報及處理程序 (1) 由第一線同仁進行初步判斷與事件分類，如可處理則填寫「資安事件通報及處理紀錄單」，將通報時間及內容描述記載於紀錄單上，並向組長說明狀況後，由組長派工；如無法處理，則由組長針對事件權責單位進行判斷後通報第二線人員。 (2) 第一線同仁應分析導致事件發生的根因，並進行矯正及預防作業。 (3) 如事件由第一線同仁逕行處理應於處理完畢後，請使用者於「資

	安事件通報及處理紀錄單」簽名確認後始可結案。 2. 事件處理完畢後，應由權責單位主管結案。 四、事件處理追蹤 1. 每年由專人將「資安事件通報及處理紀錄單」，整理後送交主管覆核後留存，並特別注意逾期尚未結案之事件。 2. 每年查核期間應針對「資安事件通報及處理紀錄單」上所發生事件進行統計分析，建議至少產生以下數據： ● 查核期間內總案件數 ● 查核期間內結案案件數 ● 查核期間內逾期結案案件數 ● 查核期間內逾期未結案案件數 ● 各類案件平均結案時間 ● 常見事件之統計分析 五、事後處理原則 1. 應定期重新審視資安事件之處理紀錄，以進行必要之改善措施。 2. 緊急處理資安事件後，應進行後續的矯正預防措施。 六、矯正及預防措施 1. 當發生下列資安事件時，需針對各事件撰寫矯正及預防措施： ● 重大或緊急事件。 ● 經常發生之一般安全事件。 ● 內部及外部稽核所發現之缺失。 ● 管理審查會議之缺失報告。 2. 矯正及預防措施之實施狀況應包含以下步驟： ● 辨識資安事件。 ● 判斷資安事件之根本原因。 ● 評估資安事件之矯正及預防處理措施。 ● 執行矯正及預防處理措施。 ● 記錄矯正及預防處理措施的執行結果。 ● 審查矯正及預防處理措施的執行結果。 3. 矯正及預防措施之實施狀況，須經本單位主管或缺失發現者 (如內部稽核時之稽核人員) 確認，以確保矯正預防措施的有效性。
控制重點	1. 負責人員應負責將事件及事件處理狀況記錄於「資安事件通報及處理

	紀錄單」之上，並隨時記錄處理過程與進度。 2. 矯正及預防措施之實施狀況，須經本單位主管或缺失發現者 (如內部稽核時之稽核人員) 確認，以確保矯正預防措施的有效性。
注意事項	無

附　件：

流 程 圖	資安事件通報及處理作業流程圖
相關表單	1. 資安事件通報及處理紀錄單。
相關法規	無
其　　他	無

■ 資安事件通報及處理作業流程圖