靜宜大學各項作業控制重點

四、營運事項

（七）資訊處理事項

作業項目	控制重點
1. 檔案及設備之安全作業	1. 機房管理： 1.1 是否制定完整之電腦機房管理制度。 1.2 電腦機房是否依據電腦機房管理辦法妥善管理。 1.3 電腦機房是否具獨立供電系統、自動穩定電壓及溫度控管等設備。 1.4 電腦機房是否嚴禁擺置易燃物品；消防設備是否定期檢測有效使用期間。 1.5 重要電腦及通訊設備是否特別防護；人員進出電腦機房之控管，是否亦經核准。 1.6 每日機房設備運作情形，是否確實檢查並作成紀錄。 2. 檔案備份： 2.1 檔案備份是否依「備份排程表」，是否確實記錄於「備份＼異地備份媒體管理表」。 2.2 檔案備份作業發現異常時，是否於「電腦主機房工作日誌」上記錄發生原因及排除方法。 2.3 檔案備份資料是否置放於安全且獨立於機房外之處所。 2.4 檔案備份資料是否定期測試其回存之可用性。 3. 安全管理： 3.1 電腦使用區域之辦公設備、地板等，是否具不易燃燒且防火功能之材質。 3.2 電源自動斷電功能是否良好、通風及空氣調節是否暢通。 3.3 逃生出口是否保持乾淨暢通、逃生路線是否明確標示，並有緊急照明裝置。 3.4 是否設置消防器材或系統因應突發狀況。 3.5 對進出電腦使用區域之敏感地區是否有足夠的管制措施。

2. 硬體修繕作業	1. 委外修繕階段-各項委外修繕案件是否依規定辦理並經核准。 2. 廠商估價是否相符市場行情。 3. 估價單是否詳細載明所使用之原物料品名、單位、數量及單價。 4. 委外修繕驗收階段：驗收人員是否於修繕單之「請修單位驗收」確實簽章，以示負責。 5. 委外修繕付款階段：核對付款金額是否符合。
3. 系統開發及程式修改作業	1. 應用系統開發及管理制度-系統開發管理制度是否完整而明確。 2. 應用系統開發及管理制度-系統開發方向是否能因應學校整體發展之需求。 3. 系統計劃、開發及管理-需求提出：系統開發前，應用系統需求規格書是否經過適當之核可及評估。 4. 系統分析-是否指派專人負責進行系統分析作業；分析人員是否與相關單位人員有充份之討論互動。 5. 系統分析人員是否針對系統之功能、流程等進行評估，並向相關人員確認系統開發設計方向之正確性。 6. 系統設計-系統開發作業是否依循需求分析結果之內容設計。 7. 系統設計-系統設計是否具整體性規劃，並整合跨單位之需求。 8. 系統發展與測試管理-程式設計、測試過程及系統程式轉換情形是否完整記錄與保存。 9. 系統發展與測試管理-系統測試環境與正式作業環境轉換所發生問題是否經適當解決。 10. 系統發展與測試管理-程式執行異常時，是否依規定之程序回報申請修改。 11. 系統運作使用管理-是否進行必要之教育訓練，並告知注意事項。 12. 系統之測試結果如已符合使用者之需求後，是否請申請人確認。 13. 系統評核管理-系統啟用後，如有執行結果不當或錯誤時，是否回饋至系統分析人員。 14. 系統分析人員是否依使用者回饋訊息，進行系統運作不當或錯誤之檢核，並會同程式設計人員修正。

	15. 系統之維護、組織與管理-使用中之系統如有修改需求，需求者是否提出修改申請，並陳相關權責主管簽審。 16. 計算機及通訊中心是否對程式修改申請進行評估。 17. 系統運作使用後，如經大幅修改測試完成時，相關文件是否一併修正或定期更新。 18. 外包業務管理-外包業務之契約內容是否週詳。 19. 與被委託單位之權責是否劃分詳盡。 20. 委外開發系統是否經過品質測試確認程序。 21. 計算機及通訊中心人力及能力不足時，外包時是否與外包公司簽訂維護合約。 22. 個人機敏資料存取管理-個人機敏資料欄位之批次存取活動是否予以記錄並保存。
4. 資料輸出入及處理作業	1. 各項資料之輸入是否評估其工作範圍、權責後，始授權執行輸入作業。 2. 對於具影響性之系統操作功能，是否設定使用者權限。 3. 應用程式是否設定自動檢核功能。 4. 資料輸入處理是否留下紀錄。 5. 當資料輸入發生錯誤時，是否立即追查原因並處理之。 6. 錯誤資料更正是否依既定程序分析錯誤屬性。 7. 資料輸出是否經過適當之核准程序處理。 8. 當輸出資料不成功或不需要時是否經適當銷毀處理。 9. 輸出資料保存是否妥當。 10. 配合個資安全維護，執行個資蒐集、處理、利用、安全維護程序。
5. 系統復原計畫及測試作業	1. 覆核是否制定書面之演練計劃。 2. 備援計劃是否完整及明確。 3. 是否訂有允許復原時間。 4. 復原程序是否訂明復原工作之執行順序。 5. 是否制訂完整且可行之書面復原計劃。 6. 是否定期測試及演練復原計劃，以確保硬體或軟體復原計劃之適用性及支援運作能力。

	7. 當硬體或軟體發生異常時，計算機及通訊中心人員是否依【資訊業務持續營運管理程序】及【資訊業務災害回復作業規範】執行。 8. 硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生，且填寫資安事件處理單及矯正與預防處理單。 9. 對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商進行復原，避免本校系統運作中斷。 10. 重置後之硬體或軟體，是否執行測試確認系統之可用性。 11. 於完成回存作業後，是否確認資料回存之完整性。 12. 計算機及通訊中心人員是否將測試結果紀錄存查。
6. 應用系統及資料存取控制作業	1. 資訊存取安全規劃，是否訂定相關偵防措施及管理辦法。 2. 使用者權限管理-是否訂定資訊存取安全程序。 3. 使用者登錄系統辨識碼及使用權限之維護程序是否依規定辦理。 4. 本校人員離職或調職時，是否立即註銷、暫停或更新使用者帳號、密碼權限。 5. 系統資料變更管理，是否以使用者權限限定資料之存取權限。 6. 系統及檔案存取-教職員工及學生使用系統及檔案是否有適當控管。 7. 經授權使用之認證及資料同步帳號、密碼權限是否予以列管保護。 8. 系統及檔案之存取使用是否留下紀錄。 9. 系統原始程式及目的程式是否分開存放。 10. 配合個資安全維護，執行個資蒐集、處理、利用、安全維護程序。