中央研究院應用系統存取控制管理要點

民國 98 年 9 月 30 日經院長核定

規定		說明
一、	中央研究院(以下簡稱本院)為推動各單位強化應用系統存取控制安全管理，依本院資訊安全規範第四點第五款之規定訂定本要點。	本管理要點法源。 電腦軟體區分為作業系統和應用系統兩部分。「應用系統」包括各單位電子郵件、資料庫、網站、行政管理系統、學術研究應用軟體系統等。
二、	本要點適用於本院應用系統帳號、通行碼、使用權限及存取紀錄等管理事宜。	
三、	帳號新增及異動管理應依下列原則辦理： (一)帳號新增及異動須經申請，並經權責人員核可後，交由系統管理人員辦理，並保留紀錄。 (二)帳號、通行碼之通知過程應有保護措施，防止被窺視竊取。 (三)單一使用者於單一系統上僅使用一個帳號，因業務或特殊原因需使用兩個以上帳號，應提出申請。 (四)人員職務異動、留職停薪或離職時應依規定辦理帳號移交或註銷，未依規定辦理者，系統管理人員得逕行停止該帳號之使用。 (五)不得共用帳號，以區分安全責任。	可另行參考「計算中心使用者帳號申請及使用注意事項」。
四、	應用系統登入管理應依下列原則辦理： (一)宜設定可開放連線之時間或連線逾時自動登出之機制。 (二)除帳號、通行碼外，應依業務需求考量是否採用其他適切之身分鑑別技術。 (三)登入作業完成後，宜顯示前一次登入成功或失敗之時間或相關訊息。 (四)限制連續登入失敗次數之上限，登入失敗次數達上限者，應暫停該帳號一定時間之登入，或	

	鎖定該帳號直到系統管理人員重新啟動。 (五)必要時限定使用者之 IP 位址。	
五、	使用者通行碼應善加設計，力求降低被破解之風險，並應妥善保管避免他人知悉。 重要應用系統之通行碼不宜連續使用超過6 個月。	可另行參考「電腦系統通行碼設計原則」。
六、	應用系統使用存取權限管理應依下列原則辦理： (一)使用者權限之申請，應由權責單位依使用者執行職務之需求，以工作所需最小權限之原則核可後，交由系統管理人員執行相關設定。 (二)未經核可之申請，系統管理人員不得進行授權作業設定。 (三)系統管理人員進行遠端維護時，應限制其經由本院核可之遠端連線來源。	
七、	重要應用系統應啟動系統紀錄功能，系統管理人員應保存系統紀錄檔並定期備份。 各系統應視其重要性及支援程度將下列事件列入紀錄： (一)系統管理人員及具備特殊權限帳號者之登入成功及失敗事件。 (二)使用者帳號異動及對通行碼檔案之讀取與變更。 (三)程式原始碼及執行碼之變更。 (四)直接進入資料庫管理系統變更資料。 (五)系統設定檔之存取及變更。	「系統支援程度」視作業系統或資料庫管理系統所能支援的日誌(log)功能而定。例如，作業系統通常都能提供第一款、第二款的日誌功能，以及第三款、第五款的變更時間；資料庫管理系統或可提供第四款的日誌功能。
八、	系統管理人員應依下列原則辦理存取控管作業查核： (一)定期辦理帳號清查。 (二)監控有無違反系統存取規定之安全事件，並定期檢視紀錄，分析其異常狀況。 (三)存取紀錄檔須另行查核。	可另行參考「計算中心使用者帳號申請及使用注意事項」。
九、	各單位開放外界連線作業之應用系統，應避免人員直接存取應用系統之資料檔，必要時得視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、代理伺服器、防火牆及安全漏洞偵測等不	

	同安全等級之技術或措施，防止資料及系統遭入侵、破壞、竄改、刪除或未經授權之存取，並記錄完整系統使用資料。	
十、	本要點經院長核定後實施，修訂時亦同。	