中央研究院資通系統電子形式軌跡資料（Log）管理要點

中華民國107年9月27日第4次院務會議審議通過
中華民國107年11月23日院長核定
中華民國109年9月17日第4次院務會議審議通過
中華民國109年12月28日院長核定

一、中央研究院（以下簡稱本院）為確保電子形式軌跡資料（以下簡稱 Log）之蒐集、處理及利用符合資通安全及資訊隱私之維護，依個人資料保護法施行細則第24條之規範，訂定本管理要點。

二、本要點所稱 Log 指在使用資通系統服務過程中，由作業系統、應用系統、資安設備、網路設備等軟硬體自動產生使用狀態之紀錄，包括但不限於使用者之存取帳號、存取時間、網路 IP 位址、使用設備代號、網路路徑等使用資通系統之紀錄。

三、本要點適用範圍為本院各單位提供或管理之資通系統。

四、本院提供或管理資通系統之各單位主管應指派負責督導資通安全業務之 Log 主管（由各單位資通安全主管或資訊室主任擔任為原則）執掌以下事務：

（一） 指派掌有資通系統帳號管理權限者為Log管理者。

（二） 受理Log調閱書面申請。

（三） 接受口頭答覆申請案之報備

（四） 監督稽核 Log 管理者落實資通系統之維運及安全管理工作。

（五） 為資通安全目的提出 Log 調閱申請。

Log 管理者，執掌以下事務：

（一） Log 之保存與稽核。

（二） 為維護資通系統安全所為之威脅分析與因應。

（三） 資安事件之調查處理。

五、各單位之 Log 應依照中央研究院資通安全管理規範實施要點進行保存。

各單位應定期依 Log 自動產生之綜合分析報告，進行例行性檢視，分析異常狀況，及早發現潛在的資安威脅，以維持系統正常穩定運作。

各單位應建立 Log 管理者之權限控管、身分認證機制。並訂定 Log 之閱覽、判讀、更改設定之作業程序規範，報院備查。

各單位發現資通安全事件時，除依中央研究院資通安全管理規範實施要點進行通報及處理。如需調閱 Log，其申請審核程序依第六點規定辦理。

六、申請調閱 Log，除法律另有規定者外，以本院人員為因應資通安全威脅所必要者為限。

為有效迅速解決資通安全威脅，Log 管理者得接受申請人以口頭申請，並得逕以口頭答覆。但有下列情形之一者，應以書面提出調閱申請：

(一) 申請閱覽或提供複製本。

(二) 不宜以口頭答覆者。

Log 管理者以口頭答覆後，Log 主管認定應以書面提出申請者，應請申請人補提書面申請。

各單位為資通安全目的有主動調閱Log必要時，應由Log主管以書面提出調閱申請。但為因應緊急資通安全之必要，得先以口頭向單位主管報請核准調閱之，並儘速補提書面申請。

本院以外之政府機關依法請求本院提供Log者，應以機關名義來函敘明法律依據及請求提供Log之特定範圍。

七、以書面申請調閱者，由Log主管報請單位主管核准得調閱之 Log 項目及內容。申請人為單位主管者，由單位副主管或最資深研究人員核准之。單位主管或 Log 主管因職務所知悉之資訊，應保守秘密。

以口頭申請並以口頭答覆者，由 Log 管理者進行審核，並儘速以書面或電子紀錄方式向 Log 主管報備。Log 主管並應定期稽核Log管理者受理口頭申請與實際提供口頭答覆之業務處理情形。

提供調閱或口頭答覆之範圍，以解決資通安全威脅所必要之最少資料為限。

調閱之 Log 涉及第三人之使用紀錄時，除應由單位主管審核外，並應通知

該第三人。

八、Log 管理者應負以下之管理責任：

（一） Log 管理者不得對 Log 進行管理權責以外之監看與分析。

（二） 書面調閱申請文件，Log資料管理者應妥善保管。

（三） 因職務所知悉之資訊，應保守秘密。

（四） 應保管調閱申請之紀錄。

（五） 所屬單位人員離職或職務調動時，立即辦理權限異動或帳號移除。

九、本院提供或管理資通系統之各單位應公告隱私權政策，聲明該管資通系統為維護系統安全將自動記錄整體或個別使用者Log之類別及其利用方式。

十、本要點經院務會議通過，院長核定後實施，修正時亦同。