中央研究院

資訊科學研究所

委外安全管理作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I314

版　　本：1.1

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件
1.1	113/10/18	資訊室			依總統府稽核改善要求，修訂伍、七、委外廠商稽核作業標題及內容。

目錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為降低資通訊業務受託者進行委託業務作業時的資通安全風險，訂定委外管理作業說明書（以下簡稱本說明書），以資遵循。

貳、依據

一、 資通安全管理法及資通安全管理法施行細則。

二、 中央研究院資通安全管理規範實施要點。

三、 ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）。

參、範圍

適用於本所委外辦理資通系統之建置、維運或資通服務之提供。

肆、權責

一、 委外作業單位：(參照本院資通安全管理規範實施要點的用詞)

(一) 擬定籌獲作業。

(二) 擬定採購招標文件。

(三) 選商作業。

(四) 委外作業管理。

二、 受託者：

執行委託單位資通系統之建置、維運或資通服務之提供。

伍、作業說明

一、 資訊業務委外處理時，應遵循政府相關法規辦理。

二、 業務委外辦理考量因素如下：

(一) 限於技術或人力無法自行辦理。

(二) 自行辦理難以滿足時效要求。

(三) 自行辦理不符成本效益。

(四) 其他相關環境條件無法配合。

三、 委外作業準備

(一) 委外作業單位依需求制訂需求書或規格書時，須依據中央研究院「資訊服務採購資安要求事項」規定納入「需求書(或規格書)資安要求項目」並估算資安經費。

(二) 應將必要的軟、硬體之安全要求列入採購需求。

(三) 研擬契約時，須採用中央研究院「資訊服務採購資安要求事項」規定之「中央研究院資訊服務採購契約範本」，並於契約規範受託者資安專業資格與能力。

(四) 招標文件應要求受託者參與該採購案之相關人員提供中央研究院資訊採購保密切結書。

四、 委外作業管理

(一) 受託者執行委外業務如有需使用本所相關資源時，應依相關規定辦理申請。

(二) 本所若需針對合約標的之資安資料保護情形進行查核監督，受託者不得以任何理由進行拒絕。

(三) 受託者人員對於系統之操作，系統業務管理者應盡監督之責，受託者人員不得任意從事非工作範圍內之操作。各系統管理者應視需要於受託者人員完成工作後檢視系統紀錄。

(四) 受託者進出機房區域，應依據本所電腦機房相關安全管理辦理。

(五) 委託單位委託辦理建置、維運資通系統或提供資通服務之受託者涉及委託單位專案之所有場域(含租借)，委託單位應定期監視與審查由受託者提供的服務、報告及記錄。

(六) 驗收或契約到期與結束時，應刪除廠商使用之相關系統帳號並請廠商銷毀所持有之委託單位資料，或依指示返還，並保留執行紀錄。

(七) 廠商因履約所取得或得知之委託單位系統或設備相關資訊須負保密責任、以「最低接觸需求」為原則，並提供保護機制。

五、 委外服務變更管理

受託者所提供之服務內容如有重大變更，應由業務承辦人依行政程序，並視需要附上相關風險評鑑之佐證資料，經分層負責規定核可後，方可

進行變更。

六、 轉包與分包

(一) 委外服務不得轉包。

(二) 若受託者再下分包委由其他廠商提供服務時，契約中須註明受託者對其下分包商必須負連帶保密責任。

(三) 受託者協議中，應考量加入包含與資通訊科技服務及其產品供應鍊相關資通安全風險之要求考慮，包括確保得到的產品功能如預期，沒有任何非預期或不需要的功能(如：後門程式、隱密通道及惡意病毒程式)。

七、 委外廠商稽核作業

(一) 委託單位須依據數位發展部資通安全署「資通系統籌獲各階段資安強化措施」規定，辦理委外廠商稽核作業。

(二) 辦理廠商稽核前，應事前規劃並編製委外廠商資通安全稽核計畫，稽核計畫應經本所資安長核定後實施，修訂亦同。

(三) 稽核後，由稽核團隊擬訂委外廠商資通安全稽核報告，經受稽廠商代表與稽核員簽署後，陳核本所資安長。受稽廠商應就資通安全稽核報告中所列缺失事項提具矯正措施或改善計畫，由本所列管並確認矯正措施之執行結果。

(四) 委外廠商資通安全稽核結果及改善作業執行情形應於本所之管理審查會議報告。

陸、參考文件

一、 資訊服務採購資安要求事項。

二、 中央研究院資訊服務採購契約範本。

三、 資訊服務採購需求書(或規格書)資安要求項目。

四、 資通系統籌獲各階段資安強化措施。

柒、使用表單

一、 委外廠商資通安全稽核計畫

二、 委外廠商資通安全稽核報告