臺北市政府資通訊業務委外作業指引

中華民國111年2月24日臺北市政府(111)府授資安字第1113003287號函訂定發布

壹、 總則

一、 臺北市政府(以下簡稱本府)為確保所屬各機關(構)(以下簡稱各機關)資通訊業務委外作業規範，特訂定本指引。

貳、 適用範圍

二、 本指引所稱資通訊業務委外作業，係指各機關委託廠商(以下簡稱受託者)辦理或提供資通訊相關之業務（以下簡稱受託業務），均應遵守本指引之規定。本指引所稱委外業務如下：

（一） 資訊服務，指提供與電腦軟體或硬體有關之服務；包括整體規劃、系統整合、系統稽核、系統管理、網路管理、軟體開發、軟體驗證、軟體維護、硬體維護、硬體操作、機房設施管理、備份與備援服務、網路服務、顧問諮詢、稽核審查、資料庫建置、資料處理、資料登錄或訓練推廣等服務。

（二） 雲端服務，指利用網路連結遠端伺服器所提供之服務；至少包括軟體即服務(SaaS) 、平台即服務(PaaS) 及基礎設施即服務(IaaS)等。

三、 統包工程契約、工程契約、財物契約、勞務契約、無償所提供或複委託者之委外作業，其受託業務包含上述資通訊相關者亦適用之。

參、 資通訊業務委外籌獲管理

四、 各機關於資通訊業務委外籌獲管理時，依下列規定辦理：

（一） 招標前應進行風險評估並依資通安全責任等級分級辦法訂定資通系統防護需求等級。

（二） 應遵循各機關對危害國家資通安全產品限制使用原則，如採購屬經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議委員會公告之陸資資訊服務業者。

（三） 應於招標文件明定執行之團隊成員不允許大陸地區廠商及陸籍人士參與，且不得採購及使用大陸廠牌資通訊產品。

（四） 機關得評估資通訊業務之風險程度與採購可行性，限制廠商所供應標的（含工程、財物及勞務）之原產地不得為大陸地區。

（五） 受託者辦理受託業務之相關程序與環境，應具備完善之資通安全管理措施或通過第三方驗證。

（六） 契約應納臺北市政府資通安全管理規定及臺北市政府資通系統安全作業指引之要求，並訂定違約及服務績效違約金。

五、 各機關與受託者簽訂契約，其內容應包含以下資料：

（一） 受託者應遵循之資通安全、保密條款及作業相關之法規要求。
（二） 各項資通安全控管要求，以明確告知受託者應遵循事項。
（三） 相關資通資產之機密性、完整性、可用性及法規性要求。
（四） 本府得保留對受託者進行資通安全稽核之權利。
（五） 其他轉包受託者及相關參與者的責任義務。

六、 受託業務若涉及個人資料蒐集、處理與利用時，受託者應遵循個人資料保護法及本府之相關規定，僅於委外服務涉及個資範圍、類別、特定目的及其期間進行處置，不得逾越其特定目的。委託關係終止或解除時，受託者應返還個人資料或刪除其持有之個人資料(含備份與暫存檔)。

肆、 資通訊業務委外建置與維運

七、 各機關於資通訊業務委外建置與維運時，應要求受託者依下列規定辦理：

（一） 禁止受託者遠端連線管理伺服器，如有遠端管理需求，應以 MDVPN 或 SSL VPN 等加密連線，一人一帳號且採取多因子認證，並僅得連線至受託者管理之主機範圍，降低重要主機可能攻擊範圍；連線及登入之相關紀錄應納入監控，有異常行為應停用帳號並進行調查。
（二） 執行業務前應簽署委外廠商執行人員保密切結書及委外廠商執行人員保密同意書。
（三） 履約及駐點相關人員應定期執行資安訓練，訓練內容應包含本府最新資安法規與政策、標準作業程序、最新資安情資、防護技巧、經驗傳承等專業訓練，以建立人員資通安全認知，提升人員資通安全水準。
（四） 所提供之軟硬體及資通系統，包含受託者內部及建置於機關機房者，均應遵循臺北市政府資通系統安全作業指引，並於查驗、驗收時檢視確認落實。
（五） 應配置資安專職人員，確認履約階段符合雙方資安管理規範。
（六） 於發生可能影響機關之資通安全事件時，應依資通安全事件通報及應變辦法所定時限，主動通知機關進行損害控制或預防措施，以避免災情擴大或遭受波及。
（七） 受託者應自行辦理資安稽核作業。

八、 受託者或受託業務如有異動時，應檢討原契約內容，必要時應重新簽訂新約，並評估資安措施之有效性，以進行必要之調整。

九、 各機關應定期使用本府訂定之受託者稽核表進行稽核，確認受託者及複委託者辦理資通安全相關工作之情形；如有缺失，應追蹤管考，並納入後續採購評估及限縮權限等風險控制措施，以降低委外辦理資通系統或服務安全威脅。若受託業務為雲端服務受託者應提

供相關資安國際認證證明。

十、 受託者提供之受託業務發生資安事件、受託者端發生重大資安事件(如：遭加密攻擊、阻斷服務攻擊等)或其他依受託者專業判斷之資安事件，應於一小時內依機關指定之方式及對象，進行資通安全事件之通報。

受託者於資安事件處理過程中，如涉及民、刑事法律行動，應進行蒐證與證據保留。於證據蒐集完成前，相關設備不應重新開機，以保全完整證據。完成資通安全事件之通報及應變程序後，受託者應提報資安事件檢討報告予機關。

伍、 附則

十一、 各機關得依業務需要，自行訂定其他執行管理規範。