資通訊產品採購資安指引

114.4.2 版

名詞定義：

- 資訊軟體：用來處理、管理和傳輸資訊的軟體工具和應用程式。
- 資訊硬體：指的是在資訊系統中用來處理、存儲、傳輸及展示資訊的設備。
- 資訊系統：涵蓋硬體、軟體、數據、人員和流程等多個方面的軟體系統。資訊系統的目的是支持和改善組織的運作和決策，用於整合和管理組織的各種業務流程，如企業資源規劃（ERP）系統、HRM 人力資源系統、網站、行動應用軟體(APP)、客製化套裝軟體等。
- 資訊服務：指提供與資訊軟硬體有關之服務，包括雲端服務、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、備援服務、網路服務、顧問諮詢、資料庫建置、資料處理、資料登錄或訓練推廣等服務。
- 資通訊產品：參考資通安全管理法第 3 條用詞定義，包含資訊軟體、資訊硬體及資訊服務等，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、伺服器、無人機、印表機、網路通訊設備、可攜式設備及物聯網設備（包括監視系統、網路電話、會議系統、電話總機系統、顯示器、影印機、門禁系統、事務機等）等。

遵循「資通訊產品採購安全規範」[1]與「禁止使用及採購大陸廠牌資通訊產品」[2]

資訊系統建置開發與維護（含 APP）

備標階段

完成下列作業流程與表單：

(1) 資通系統安全等級評估表
- ✓承辦單位核定資訊系統安全等級（普、中、高）

(2) 廠商資安管理作業自評表[3]
- ✓為評選時，廠商服務建議書納入資安管理作業自評內容
- ✓指商採購，請廠商於請購階段交付

履約階段

(3) 委外廠商團隊成員名冊暨保密同意書與切結書
- ✓廠商應簽署保密協定

(4) 資通安全聯絡人員表
- ✓廠商須提供專案資通安全事件通報窗口及聯繫方式

(5) 未使用大陸廠牌切結書
- ✓廠商應簽署非大陸廠牌與服務協定

(6) 資料所在地及跨境傳輸切結書（雲端服務適用）
- ✓廠商提供之資訊軟硬體設備或勞務資料存取、儲存、備份及備援等作業，其實體設備所在地及資料傳輸非跨境大陸

(7) 資通系統資安防護基準要求與查核表
- ✓廠商須依資通系統安全等級所評估普、中、高等級，逐項檢視並執行該等級所要求之防護基準控制措施。

(8) 安全性檢測與弱點修補作業
- ✓資訊系統開發階段：上線前應完成網頁弱點掃描、源碼檢測
- ✓資訊系統維護階段：應每二年至少 1 次完成網頁弱點掃描
- ✓此項目可能衍生費用，請編列預算執行

(9) 備份機制明細表
- ✓資訊系統安全為普中高等級，廠商須完備份機制建置

(10) 備份測試查核表
- ✓廠商與資訊系統承辦單位應配合營運持續演練作業、備份測試作業
- ✓核心系統應每二年進行演練作業並驗證測試所備份資料復原後是否能正常運作；非核心系統應至少完成備份還原測試

(11) 委外廠商查核項目表
- ✓承辦單位對委外廠商服務之監視與審查，廠商應配合完成相關查核表格，並檢附佐證資料

(12) 資料返還、刪除、銷毀切結書

※(3)至(6)、(12)文件廠商須於契約生效後 10 個工作天內交付
※(7)至(11)文件廠商最晚須於履約期限屆至前交付

承辦單位	資通訊產品採購
承辦單位	遵循「資通訊產品採購安全規範」
承辦單位	資通系統經資安長核定防護普、中、高等級
採購與承辦單位	採購流程
承辦單位	履約管理
承辦與資訊單位	相關文件 承辦窗口留存

電腦硬體、資通訊設備(凡有接上網路皆屬)、周邊設備

禁止採購大陸廠牌產品（如小米、華為、TP-Link）

於契約生效後 10 個工作天內交付

(1) 未使用大陸廠牌切結書

(2) 委外廠商團隊成員名冊暨保密同意書與切結書
- ✓如提供維護管理設定等服務須附

套裝軟體（含 APP）

禁止採購大陸廠牌產品（如 EaseUS）

於契約生效後 10 個工作天內交付

(1) 未使用大陸廠牌切結書

(2) 委外廠商團隊成員名冊暨保密同意書與切結書
- ✓如提供維護管理設定等服務須附

雲端服務

禁止採購落地於中國之雲端服務（如阿里雲）

於契約生效後 10 個工作天內交付

(1) 廠商資安管理作業自評表[3]

(2) 資通安全聯絡人員表

(3) 委外廠商團隊成員名冊暨保密同意書與切結書

(4) 未使用大陸廠牌切結書

(5) 資料所在地及跨境傳輸切結書

(6) 資料返還、刪除、銷毀切結書

原則：
- ✓雲端服務如廠商提供維護管理設定等服務，須檢附(1)~(6)文件（如中心 AWS、中華電信 Hicloud 服務採購，且廠商提供代管服務）

資訊人力服務

禁止大陸籍人士

於契約生效後 10 個工作天內交付

(1) 廠商資安管理作業自評表[3]

(2) 委外廠商團隊成員名冊暨保密同意書與切結書

(3) 未使用大陸廠牌切結書

(4) 資料返還、刪除、銷毀切結書

(5) 委外廠商查核項目表

註[1]：依核定「資通訊產品採購安全規範」辦理，相關表單於 https://drive.google.com/drive/folders/1qcx50yR4ae-_ewISwor7-omvxMVpNwqC?usp=sharing 下載。

註[2]：依「行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函」，禁止使用及採購大陸廠牌資通訊產品。

- 常見大陸廠牌以下提供參考，包括但不限於：Boox、CREALITY、CRF PLASMA、CZUR、Dahua(大華)、Dimension、DJI(大疆)、DLAB、FOCUCY、Foscam、FOXTECH、HARMANKARDON、Hikvision(海康威視)、Hisense(海信)、Huawei(華為)、Hunan Kecheng Instrument and equipment、HYREAD、INNO3D、Insta360、Korno、Livox、LREALITY(創想)、MEIZU(魅族)、Mercusys(水星)、MI(小米)、Micsig、Mind Sensor(意念精靈)、Nanhua、Nubia(努比亞)、OBSBOT、OPPO、OPT Machine Vision Tech、Partulab(百力博)、QTS、REALME(真我)、RIGOL、RisingCam、RMY、Royal(賓利皇家)、Seeed Studio、SEGWAY、Snapmaker、Sugar、Tenda、TLC、TOTOLINK、TP-Link(普聯)、vivo、YUDIAN、ZOTAC(索泰)、中興通訊、嘉兆、映眾、步進電機、石頭科技、螞蟻源科學儀器、銳太、騰達...等廠牌。

註[3]：

- 本項係依據資通安全管理法第 9 條與資通安全管理法施行細則第 4 條規定，於委外辦理資通系統之建置、維運或資通服務之提供，應考量廠商之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。
- 招標方式以評選辦理採購，須於評選須知中請廠商於服務建議書納入廠商資安管理作業自我評估表。
- 招標方式以指商採購，請廠商於請購階段交付。