資通訊委外安全管理要求

112.01.12

購案標的：PEOPO 雲端系統平台租賃及維護案

一、廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本會資通安全管理及保密相關規定。

二、廠商履約人員國籍不得為中國籍，且所使用之資通設備、服務、軟體及元件不得為中國所有（大陸品牌）。

三、廠商辦理本專案之相關程序、人員、設備及環境，應具備完善之資通安全管理措施或通過第三方驗證。

□ 廠商應通過第三方驗證（ISO 27001 最新可被驗證版本）。第三方驗證機構須經財團法人全國認證基金會 TAF 認可 。

■ 廠商辦理本專案之相關程序、人員、設備及環境須具備完善之資通安全管理措施。

四、廠商於本專案應指定專案管理人員，專案成員應具備該領域之專業證照，以保證履約交付內容之品質，並配置「資通安全專業人員」，以及提供資通安全專業人員擁有之資通安全專業證照（數位發展部資通安全署公告之資通安全專業證照清單之一）或具有類似業務經驗證明。

五、■本專案不得複委託（分包或轉包）；□本專案得複委託，複委託之受託者應具備與本專案廠商相同之完善資通安全管理措施或通過第三方驗證。

六、□本專案業務涉及國家機密，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

七、□廠商應提供本專案資通系統（客製化）之安全性檢測證明，其檢測工具不得為自由軟體，且需提供檢測工具名稱、版本及原始報告，以及確認檢測時之弱點資料庫已更新至最新版本（檢測報告必須載明檢測日期及檢測工具名稱、版本，以及弱點資料庫更新日期）。

檢測項目如下：

□ 系統主機弱點掃描

□ 網頁弱點掃描

□ 滲透測試

□ 原始碼檢測

承前項：□本專案資通系統為本機關核心資通系統或本專案金額達新臺幣一千萬元（含）以上，應由第三方進行安全性檢測及提供檢測報告，第三方機構應為現行「電腦軟體共同供應契約」之資通安全服務暨資訊服務廠商，且檢測項目須與廠商「電腦軟體共同供應契約」合格項目相符，所提供之檢測報告規格、要求亦須符合「電腦軟體共同供應契約」要求。

八、本專案資通系統開發與維護如使用第三方軟體或元件，應提供第三方元件清單（包含版本及是否可以持續更新等資訊），並說明其來源與授權證明。

九、■廠商應確實執行組態管理(Configurat ion Management)，以確保系統之完整性及一致性。

十、本專案標的涉關鍵基礎設施(或本機關指定之設施)，廠商及分包廠商之履約人員於進場或參與工作前，應提出 3 個月內核發之「警察刑事紀錄證明」（外國人應提出該國籍政府核發之類似文件，並經公證或認證。但申請入國簽證時，已備行為良好之證明文件者除外）；其證明內容應記載無犯罪紀錄，並經機關審核同意，始得進場或參與工作。屬臨時性進場者（例如送貨司機及其隨車人員）得免提送上開證明文件，但應接受本機關或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。

十一、廠商於執行本專案及保固服務期間，若知悉或發生資通安全事件時（含本專案範圍及廠商內部管理範圍），應於 1 小時內通知本機關及採行補救措施。

十二、本專案（含保固）終止或解除時，廠商應確返還、移交、刪除或銷毀履行契約而持有之資料，並提供切結書與說明資料之刪除或銷毀方式。

十三、於本專案（含保固）期間，本會得視需求或發生可能影響本專案之資通安全事件時，對廠商及分包廠商實施現場實地資安稽核，稽核範圍為本專案相關之程序、人員、設備及環境，廠商不得拒絕。稽核結果若不符合本專案約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本會通知後應於期限內完成改善，未依限完成者，依契約違約條款辦理。

委外服務資料返還及銷毀切結書

執行項目	□資料返還 □資料銷毀		
案名			
單位(公司)名稱			
原因	□契約終止/解除 □其他_____		
資料清冊/說明			
資料格式	□紙本 □電子 □其他_____	資料數量	
執行時間	年　月　日	執行地點	□ □資料使用單位辦公室 □其他_____
執行方式	□資料返還 □實體破壞(碎紙/水銷/火銷) □資料刪除/格式化 □其他_____		
執行紀錄	※請提供佐證資料，如：拍照、截圖、委外處理契約…		
執行人員	年　月　日	本會監審人員	年　月　日
備註：若資料清冊/說明過多，附於此表單後面陳核即可			

本單位(公司)已依契約規定，□返還/□銷毀受託業務所持有之機敏資訊或個人資料。
若違反本切結書之規定，致造成機關或第三者之損害或賠償，本單位(公司)願負相關法律及賠償責任。

此致

財團法人公共電視文化事業基金會

資料使用單位：
負　責　人：
地　　址：

中　華　民　國　　年　　月　　日

公共電視文化事業基金會資通訊安全管理基本要求

1. 廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本會資通安全管理及保密相關規定。
2. 廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
3. 廠商履約人員國籍不得為中國籍，且所使用之資通設備、服務、軟體及元件不得為中國所有（大陸品牌），本案採購項目若屬可轉包分包者，廠商不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。
4. 廠商承諾執行本專案之相關程序、人員、設備及環境，應具備完善之資通安全管理措施或通過第三方驗證，前述第三方驗證機構須經財團法人全國認證基金會 TAF 認可。
5. 廠商提供本會服務時，如使用開源軟體，應依該開源軟體之授權範圍，授權本會利用，並以執行檔及原始碼共同提供之方式交付予本會使用，廠商並應交付開源軟體清單（包括但不限於：開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文）。
6. 廠商應提供本專案資通系統（客製化）之安全性檢測證明，且需提供檢測工具名稱、版本及原始報告，以及確認檢測時之弱點資料庫已更新至最新版本（檢測報告必須載明檢測日期及檢測工具名稱、版本，以及弱點資料庫更新日期）。檢測項目由本會依個案規模另行指定之。
7. 廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，提出安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商於上線前並應清除正式環境之測試資料與帳號及管理資料與帳號。
8. 廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合本會對系統品質及資通安全的要求。
9. 廠商提供服務，如違反資通安全相關法令、知悉本會或廠商發生資安事件時，均必須於 1 小時內通報本會，提出緊急應變處置，並配合本會做後續處理；必要時，得由資通安全管理法主管本會於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。
10. 履約標的涉關鍵基礎設施(或本會指定之設施)，廠商及分包廠商之履約人員於進場或參與工作前，應提出 3 個月內核發之「警察刑事紀錄證明」（外國人應提出該國籍政府核發之類似文件，並經公證或認證。但申請入國簽證時，已備行為良好之證明文件者除外），或出具委託書由本會代為申請；其證明內容應記載無犯罪紀錄，並經本會審核同意，始得進場或參與工作。屬臨時性進場者（例如送貨司機及其隨車人員）得免提送上開證明文件，但應接受本會或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督

管理。廠商及分包廠商之履約人員執行工作，應接受本會或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。

11. 於本專案（含保固）期間，本會得視需求或發生可能影響本專案之資通安全事件時，對廠商及分包廠商實施現場實地資安稽核，稽核範圍為本專案相關之程序、人員、設備及環境，廠商不得拒絕。稽核結果若不符合本專案約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本會通知後應於期限內完成改善，未依限完成者，依契約違約條款辦理。
12. 本專案（含保固）終止或解除時，廠商應確返還、移交、刪除或銷毀履行契約而持有之資料，並提供切結書與說明資料之刪除或銷毀方式。