

委外採購資安事項檢核表

[資通系統名稱：_____；系統防護分級：_____ (普、中、高)]

序號	適用性	項目	契約書或規格書中加註(請於 確認欄位標示寫在哪)	參考(填寫)文件	確認 (V)
1	必填 (法遵性)	廠商是否配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員	廠商應配置至少1名資通安全專業(責)人員且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗。	資通系統籌獲各階段資安強化措施執行檢核表填寫說明書	
2	必填 (法遵性)	委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證		資訊服務採購契約範本	
3	必填 (法遵性)	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料	契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之，並保留執行紀錄。	資訊服務採購契約範本	
4	必填 (法遵性)	法遵性事項相關罰則		資訊服務採購契約範本	
5	必填	委外廠商之資通安全責任及保密規定(切結書)		(1) 資訊服務採購契約範本 (2) 確認廠商後，請填寫 本校委外廠商保密切結書 [協同平台 /ISMS 專區 /ISO27001/四階文件]	
6	必填	廠商於本專案相關資安事件之管理、通報及處理情形	廠商提供服務，如違反資通安全相關法令或發生資安事件時，需配合學校做後續處理。	資訊服務採購契約範本	
7	必填	涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。	廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。	資訊服務採購契約範本	
8	必填	採購標的不得使用大陸廠牌資通訊產品		本校已於110年底全面禁用	

				大陸廠牌資通訊產品	
9	選填	委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明	1. 求委外廠商提供資通系統之安全性檢測證明，請加註以下： 請提供資通系統之安全性檢測證明。 2. 如不加註請於 <u>確認</u> 欄位標示：另案處理。	資訊服務採購契約範本 (如同一廠商有執行困難，可另案辦理)	

承辦人：

承辦單位資安種子人員：

承辦單位主管：

一、 投標須知範本(1120104修正) (請參考說明並勾選)

序號	必填/選填	條文內容	說明	完成 請打勾 (V)
----	-------	------	----	------------------

序號	必填/選填	條文內容	說明	完成 請打勾 (V)
1	選填(第3-5頁)	<p>十六、本採購：</p> <p><input type="checkbox"/> (1) 適用我國締結之條約或協定；其名稱為：</p> <p><input type="checkbox"/> 下列外國廠商可以參與投標：</p> <p>1. 國家或地區名稱：_____ (未列明者即不允許)</p> <p>2. 是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)</p> <p><input type="checkbox"/> 是 <input type="checkbox"/> 否</p> <p><input type="checkbox"/> (2) 不適用我國締結之條約或協定，外國廠商：</p> <p><input type="checkbox"/> 不可參與投標。但我國廠商所供應<u>標的(含工程、財物及勞務)</u>之原產地得為下列外國者：</p> <p>1. 國家或地區名稱：_____ (未列明者即不允許)</p> <p>2. 是否允許供應大陸地區標的：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)</p> <p><input type="checkbox"/> 是 <input type="checkbox"/> 否</p> <p><input type="checkbox"/> 下列外國廠商可以參與投標：</p> <p>1. 國家或地區名稱：_____ (未列明者即不允許)</p> <p>2. 是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)</p> <p><input type="checkbox"/> 是 <input type="checkbox"/> 否</p> <p>(3) 廠商所供應整體標的之組成項目(例如製成品之特定組件、工程內含之材料與設施)，其不允許使用大陸地區產品之項目：。</p> <p>(4) 本採購就取得或使用無人機部分應符合下列條款</p>	<p>1、採購案如適用我國締結之條約或協定者，針對「是否允許大陸地區廠商參與」，應勾選「否」(亦可不勾選)。</p> <p>2、採購案如不適用我國締結之條約或協定者，針對外國廠商： (1) 如勾選「不可參與投標。但我國廠商所供應<u>標的(含工程、財物及勞務)</u>之原產地得為下列外國者」，針對「是否允許供應大陸地區標的」，請各機關依行政院公共工程委員會107年12月20日工程企字第1070050131號函釋，視其個案特性及實際需要逕行評估是否勾選「否」(亦可不勾選)。 (2) 針對「是否允許大陸地區廠商參與：(未勾選者即不允許；如允許者，須符合兩岸進口及貿易往來相關規定)」，應勾選「否」(亦可不勾選)。</p> <p>3、增訂第(4)點機關採購取得或使用無人機之通案性規範(如屬無人機採購，請勿刪除)，就取得或使用無人機部分應符合條款(與招標文件其他條款有不一致者，本條款優先適用)。</p>	

序號	必填/選填	條文內容	說明	完成 請打勾 (V)
		<p>(與招標文件其他條款有不一致者，本條款優先適用)</p> <p>(4-1)不允許大陸地區廠商、第三地區含陸資成分廠商、在臺陸資廠商及經濟部投資審議委員會公告之陸資資訊服務業者參與。且符合下列規定：</p> <p>(4-1-1)屬機關取得財物者，廠商所供應標的，應符合相關目的事業主管機關之規範，整機不得為大陸廠牌。另不允許使用大陸地區製造或大陸廠牌之組件：。</p> <p>[註：機關有特殊需求者，例如未來使用情境涉高風險或關鍵基礎設施，請妥適訂定]</p> <p>(4-1-1-1)廠商履約所供應之無人機，除依遙控無人機管理規則第17條規定於交通部民用航空局登錄外，並應經無人機主管機關（交通部）及資通安全主管機關（數位發展部）認可之專業單位資安檢測通過（具有軟硬體不受干擾入侵、且無後門傳輸資料），並持有該單位核發之資安檢測合格證明；具射頻功能且屬國家通訊傳播委員會公告「應經核准之電信管制射頻器材」者，應取得該會核發之審驗證 3 修正條文現行條文說明。</p> <p>(4-1-1-2)其他：_____。</p> <p>(4-1-2)屬機關取得服務者，廠商履約人員不得為大陸籍人士，與提供服務直接相關而必須使用之設備、器材、軟體等，應符合相關目的事業主管機關之規範，整機不得為大陸廠牌。</p> <p>(4-1-2-1)廠商履約所使用之無人機，除依遙控無人機管理規則第 6 條及第 17 條規定於交通部民用航空局註冊登錄外，並應經無人機主管機關(交通部)及資通安全主管機關（數位發展部）認可之專業單位資安檢測通過（具有軟硬體不受干擾入侵、且無後門傳輸資料）並持有該單位核發之資安檢測合格證明；具</p>		

序號	必填/選填	條文內容	說明	完成 請打勾 (V)
		<p>射頻功能且屬國家通訊傳播委員會公告「應經核准之電信管制射頻器材」者，應取得該會核發之審驗證明。</p> <p>(4-1-2-2)無人機操作人，均應具民航局核發之合格專業操作證。</p> <p>(4-1-2-3)群飛活動應通過無人機飛行場域資通安全防护評估與檢測；飛經紅區者，其飛行計畫須經交通部及(或)活動所在之地方政府審核通過。</p> <p>(4-1-2-4)法人應訂定作業手冊，經民航局能力審查核准，並經民航局及(或)地方政府同意飛航活動申請。</p> <p>(4-1-2-5)其他：_____。</p>		
2	選填(第12頁)	<p>六十四、投標廠商之基本資格及應附具之證明文件如下</p> <p><input type="checkbox"/>本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。(上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議委員會網站 http://www.moeaic.gov.tw/)。(註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第3條規定，妥適考量本須知第16點之勾選)。</p> <p><input type="checkbox"/>本採購內容涉及國家安全，不允許大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與。(註：適用條約或協定之採購案，如勾選本項者，請依 GPA 第3條規定，妥適考量本須知第16點之勾選)</p>	<p>1、採購案如屬具敏感性或國安(含資安)疑慮之業務範疇，請參考以下 (https://www.moeaic.gov.tw/download-file.jsp?do=BP&id=ZbdrLAtDiew=)，應勾選本項，以限制大陸地區廠商、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參與投標。</p> <p>2、採購案如涉及國家安全，應勾選本項，以限制大陸地區廠商、第三地區含陸資成分廠商及在臺陸資廠商參與投標。</p>	

二、 資訊服務採購契約範本(111.04.29) (請參考說明並勾選)

序號	必填/選填	檢核項目	說明	完成
----	-------	------	----	----

				請打勾 (V)
1	選填(第4頁)	<p>第二條 履約標的</p> <p>(四)廠商應給付之標的及工作事項(由機關於招標時載明)</p> <p><input checked="" type="checkbox"/>資訊業務線上服務</p> <p>2. 廠商提供資訊業務線上服務，除契約另有約定外，應於契約約定時間內提出資訊業務線上服務建議書，就資訊業務線上服務具體範圍、服務水準、測試方式、資通安全管理機制及防護措施等向機關提出建議。上述建議書之內容，不得減損契約約定事項，並經機關核定後執行。如有減損者，無效。</p>	<p>如該採購案履約標的包含資訊業務線上服務，則應要求其提報之服務建議書內容應包含資通安全管理機制及防護措施。 如有資訊線上服務應勾選本項</p>	
2	必選(第15頁)	<p>第八條 履約管理</p> <p>(二) 契約執行期間</p> <p>1. 工作計畫 (或建議書):</p> <p>(1)廠商應於得標後○○日 (由機關於招標時載明; 未載明者, 20日) 提出工作計畫 (或建議書)</p> <p><input checked="" type="checkbox"/>資通安全及保密之計畫。</p>	<p>應勾選本項(資通安全及保密之計畫)，要求廠商於得標後，所提出工作計畫 (或建議書)，應包含資通安全及保密之計畫。</p>	
3	必選(第17頁)	<p>第八條 履約管理</p> <p>(三)廠商提供服務之團隊</p> <p>4. 廠商團隊成員應於到任當日，將已簽署之以下文件提交機關： <input checked="" type="checkbox"/>附件 保密同意書/保密切結書 <input type="checkbox"/>附件 由所屬公司享有著作財產權與著作人格權同意書 <input type="checkbox"/>附件 適任性查核同意書(受託業務涉及國家機密者)</p>	<p>1、應勾選第1項(保密同意書/保密切結書)，要求廠商團隊成員簽署並提交保密同意書/保密切結書 2、如採購案涉及系統開發設計，則第2項亦應勾選 3、如採購案涉及國家機密者，則第3項亦應勾選</p>	
4	選填(第23頁)	<p>第八條 履約管理</p> <p>(二十三)廠商履約內容涉及資通安全者，應符合下列國家標準(由機</p>	<p>請依採購案之性質，建議勾選合適選項，如要求廠商應符合CNS27001[資訊技術-安全技術</p>	

		<p>關於招標時載明)：</p> <p>.....</p> <p><input type="checkbox"/>CNS 27001；</p> <p><input type="checkbox"/>CNS 27018；</p> <p>■其他：廠商應配置至少1名資通安全專業(責)人員且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗。</p>	<p>-資訊安全管理系統-要求事項]、CNS 27018[資訊技術-安全技術-公用雲PII處理者保護個人識別資訊(PII)之作業規範]或其他資通安全管理措施。</p> <p>註：CNS27001類似 ISO27001的中華民國國家標準。</p>																				
5	必填(第23頁)	<p>第八條 履約管理</p> <p>(二十四) 其他(由機關視個案實際需要者於招標時載明)：</p> <p>...</p> <p>■<u>本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。</u></p>																					
6	必填(第33頁)	<p>第十五條 違約及服務績效違約金</p> <table border="1"> <thead> <tr> <th>評估項目</th> <th>評斷方式</th> <th>要求基準</th> <th>違約金計點</th> </tr> </thead> <tbody> <tr> <td>資安指標</td> <td>對於所維護之系統，未於規定期限取得認證日數</td> <td>每次認證超過期限</td> <td>每逾○○日計○點</td> </tr> <tr> <td></td> <td>知悉發生資安事件之通報、損害控制或復原作業時效</td> <td>應於1小時內通知機關(或接獲機關通知1小時內)，並採取適當之應變措施</td> <td>每逾○○小時計○點 (必填項目，請訂定罰點)</td> </tr> <tr> <td></td> <td>完成損害控制或復原作業之時效</td> <td>應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業</td> <td>每逾○○小時計○點 (必填項目，請訂定罰點)</td> </tr> <tr> <td></td> <td>調查及處理資安事件之時效</td> <td>完成損害控制或復原作業後，應於1個月內送交</td> <td>每逾○○日計○點 (必填項目，請訂定罰點)</td> </tr> </tbody> </table>	評估項目	評斷方式	要求基準	違約金計點	資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計○點		知悉發生資安事件之通報、損害控制或復原作業時效	應於1小時內通知機關(或接獲機關通知1小時內)，並採取適當之應變措施	每逾○○小時計○點 (必填項目，請訂定罰點)		完成損害控制或復原作業之時效	應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業	每逾○○小時計○點 (必填項目，請訂定罰點)		調查及處理資安事件之時效	完成損害控制或復原作業後，應於1個月內送交	每逾○○日計○點 (必填項目，請訂定罰點)	<p>為改善廠商於資安事件之管理、通報及處理情形，增訂廠商應依契約辦理資安事件之通報應變等項目及基準，及未依約辦理之計點方式。</p>
評估項目	評斷方式	要求基準	違約金計點																				
資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計○點																				
	知悉發生資安事件之通報、損害控制或復原作業時效	應於1小時內通知機關(或接獲機關通知1小時內)，並採取適當之應變措施	每逾○○小時計○點 (必填項目，請訂定罰點)																				
	完成損害控制或復原作業之時效	應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業	每逾○○小時計○點 (必填項目，請訂定罰點)																				
	調查及處理資安事件之時效	完成損害控制或復原作業後，應於1個月內送交	每逾○○日計○點 (必填項目，請訂定罰點)																				

			調查、處理及改善報告（或協助機關調查處理）			
		機關資料之機密性及完整性	機關擁有之敏感資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致機關敏感資料外洩或遭竄改時，按受影響資料筆數，每筆計○點/按次數計○點 (如有機敏個資，請訂定罰點)		
		個人資料之機密性及完整性	機關所擁有之個人資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致機關個人資料外洩或遭竄改時，按受影響資料筆數，每筆計○點/按次數計○點 (如有個資，請訂定罰點)		
7	選填(第39頁)	<p>(十七)資通安全責任： ...</p> <p>本案金額達新臺幣一千萬元以上，廠商交付之軟硬體及文件，應接受委託機關或其所委託之第三方進行安全性檢測：.....（其項目由機關於招標時載明）。</p>			<p>廠商交付之軟硬體應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；採購金額達新臺幣一千萬元以上，廠商應接受委託機關或其所委託之第三方進行安全性檢測。</p>	
8	請勿刪除 必填(第39頁)	<p>第十六條 權利及責任 (十七)資通安全責任： 3. 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還或移交之，並保留執行紀錄。</p>				
9	請勿刪除	<p>第十六條 權利及責任</p>				

	必填(第39頁)	(十七)資通安全責任： 5. 廠商提供服務，如違反資通安全相關法令、知悉機關或廠商發生資安事件時，均必須於1小時內通報機關，提出緊急應變處置，並配合機關做後續處理；必要時，得由資通安全管理法主管機關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。		
--	-----------------	---	--	--