檔　　號:
保存年限:

行政院公共工程委員會 函

地址：110207 臺北市信義區松仁路3號9樓
承辦人：游子熠
聯絡電話：02-87897621
傳真：02-87897604
E-mail：ziyi@mail.pcc.gov.tw

受文者：教育部

發文日期：中華民國112年9月25日
發文字號：工程企字第1120022701號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨 (360000000G_1120022701_doc2_Attach1.pdf、360000000G_1120022701_doc2_Attach2.pdf)

主旨：檢送本會與數位發展部研訂之「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」及「資訊服務採購作業指引」，請查照並轉知所屬（轄）機關。

說明：

一、各機關之資訊、資安事項多採委外辦理，而資訊科技變遷快速，各機關落實資通安全管理遭遇挑戰，為協助各機關即時有效強化資通安全防護及妥適辦理資訊服務採購，本會與數位發展部、資訊服務、資通安全產業界及相關公協會合作研訂旨揭文件，並經該部於112年9月18日同意；其中「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」將納為本會資訊服務契約範本之附件，由機關視個案特性將所列資安事項納入契約辦理。

二、考量機關按上述一覽表辦理，廠商應配合調整，為使廠商有適切時間因應，該表之資料或系統類型屬普級部分之資安要求訂於明年3月1日正式施行，中、高等級則訂於明年8

1120095418 收文日期:112/09/26

月1日正式施行。

三、另為強化機關資訊服務採購需求明確、合理編列費用及減少履約爭議，本會訂定「資訊服務採購作業指引」，從採購全生命週期提醒機關辦理資訊服務採購應注意事項，除配合前述日期開始施行之部分外，自即日起即可作為辦理資訊服務採購之作業指引。

正本：總統府第三局、國家安全會議秘書處、行政院秘書長、立法院秘書長、司法院秘書長、考試院秘書長、監察院秘書長、國家安全局、行政院各部會行總處、直轄市政府、直轄市議會、各縣市政府、各縣市議會、各鄉鎮市公所

副本：全國政府機關電子公布欄、台灣美國商會、台北市日本工商會、歐洲在臺商務協會、台北韓國貿易館、法國工商會、中華民國資訊軟體協會、台北市電腦商業同業公會、本會各處室會組、企劃處（網站）（均含附件）

2023/09/25 16:59:19

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

雲端微服務（SaaS）套裝型							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
		提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		身分鑑別/傳輸機密性與完整性	廠商提供機關帳號控管措施	◎	◎	◎	
			廠商提供機關資料傳輸措施	◎	◎	◎	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求參考

112年9月25日

雲端微服務（SaaS）套裝型	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

雲端微服務（SaaS）辦公室生產力工具 （含郵件、行事曆、雲端硬碟、即時通訊等）							
類型		項目	子項	資料或系統類型 高	中	普	說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
		提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		傳輸機密性與完整性	廠商提供機關資料傳輸措施	●	●	●	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求參考

112年9月25日

雲端微服務（SaaS）辦公室生產力工具	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告乙項，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		防惡意軟體	靜態分析	●	●	●	
			動態沙箱分析	●	●	◎	
		防惡意連結	靜態分析	●	●	●	
			動態沙箱分析	●	●	◎	
		防釣魚郵件	釣魚郵件過濾	●	●	●	
			身分偽冒辨識(anti-spoofing)	●	●	◎	
		資料與個資安全	資料分類與標籤	●	●	●	
			資料加密與存取控制	●	●	◎	
			資料外洩防護	●	●	◎	
			未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	
		身分驗證與存取控制	多因子認證	●	●	●	
			零信任：身分鑑別/設備鑑別/信任推斷	●	●	◎	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

既有雲端微服務（SaaS）客製化需求更版							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
既有雲端微服務（SaaS）客製化需求更版	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告乙項，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

		廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

雲端平台(PaaS或IaaS)							
類型		項目	子項	資料或系統類型			說明：
				高	中	普	1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級以上。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時，▲-依委託機關資通安全責任等級辦理，導入方式應依機關要求及個案需求辦理，得納入本案或另於他案採購(經確認納入他案辦理者，本案免辦)。 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
		提供平台服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	
			廠商不得為大陸地區廠商第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		弱點管理	雲端應用系統平台具備定期檢視PaaS 之應用、組件或 Web 服務是否存在漏洞並進行更新修補	●	●	●	
		存取控制	雲端應用系統平台提供帳號安全認證、權限管理、網路安全傳輸及遠端存取控管佐證	●	●	◎	
			須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制	●	●	◎	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	
		營運持續計畫	檢視廠商平台營運持續、資料復原計畫及執行情形	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求項目一覽表

112年9月25日

雲端平台(PaaS或IaaS)	資通安全項目	變更管理/安全管理	雲端應用系統平台具備變更管理制度	●	●	◎	
			雲端應用系統平台具備設定安全管理制度	●	●	●	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	
			雲端應用系統平台內如存有機密或個人資料應依相關法令強化資料安全防護措施	●	●	●	
		資安防護建置持續監控	資安監控(SOC)機制，廠商須提供 7x24 小時全天候監控	▲	▲	▲	
			須提供資安事件應變服務(Emergency Response Service)	▲	▲	▲	
			具備相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制(DDoS 防護服務、防毒、防火牆、IPS/IDS、WAF、APT等)	▲	▲	▲	
			導入端點偵測與回應機制(Endpoint Detection and Respons, EDR)	▲	▲	▲	
			導入VANS (Vulnerability Alert and Notification System, VANS)	▲	▲	▲	
			導入GCB(Government Configuration Baseline)	▲	▲	▲	如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。
		資安演練	DDoS (Distributed Denial of Service)攻防演練	◎	◎	◎	涉及重要對外服務之系統建議評估辦理。
			入侵與攻擊模擬 (Breach and Attack Simulation)演練	◎	◎	◎	涉及關鍵資訊基礎設施之系統建議評估辦理。
			紅藍隊演練	◎	◎	◎	
		資安檢測	主機弱點掃描	●	●	●	該服務屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測。
			網站弱點掃描	●	●	●	
			滲透測試掃描(由檢測人員測試雲端服務是否具備TLS v1.2以上安全通訊協定)	●	◎	◎	
			雲端服務之APP取得行動應用 App 基本資安標章	●	●	◎	
			資安健診	●	●	●	依委託機關需求執行資安檢測，或依機關規劃另案配合執行。

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

資訊系統規劃服務							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
資訊系統規劃服務	資通安全項目	提供服務商	不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		資訊服務類規劃標需納入資安政策	符合機關資訊安全要求規範 1.政府機關：資通安全管理法含子法 2.關鍵基礎設施提供者：國家關鍵基礎設施安全防護指導綱要、關鍵資訊基礎設施資安防護建議 3.金融機構：參照金融監督管理委員會針對銀行、壽險、產險、證券、期貨、保險經紀人、保險代理人相關資安規範 4.教育單位：教育部資通安全管理實施要點、教育體系資通安全責任等級分級作業規定(草案)、教育體系資通安全暨個人資料管理規範、教育部所屬機關及各級公私立學校資通安全工作事項、國立大專校院資通安全維護作業指引、教育部所管特定非公務機關資通安全管理作業辦法 5.醫療院所：基層醫療院所資安防護參考指引	●	●	●	

各類資訊(服務)採購之資通安全基本要求參考一覽表

112年9月25日

資訊安全類規劃服務							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
資訊安全類規劃服務	資通安全項目	提供服務商	不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	
		審視機關資安規劃	機關已有無法修復之高風險或發生資通安全事件第三級級第四級時，依據機關現況及限制，參考NIST Cybersecurity Framework協助機關規劃資安整體強化措施	●	●	●	

各類資訊(服務)採購之共通性資安全基本要求參考一覽表

112年9月25日

應用軟體或系統開發服務							
類型		項目	子項	資料或系統類型			說明：
				高	中	普	
		提供服務商	具備完善之資通安全管理措施	●	●	●	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	◎	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			須具備IEC 62443 資安檢測實驗室（CBTL）資格	◎	◎	◎	
			須具備發佈CVE的資格及能力	◎	◎	◎	
			開發系統導入安全軟體發展生命週期(Secure Software Development Life Cycle, SSDLC)	◎	◎	◎	提請機關資安長確認廠商所開發之系統是否有導入必要。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		符合國際標準規範	協助系統導入及取得CNS27001及ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準驗證	◎	◎	◎	依資通安全責任等級分級辦法附表一至六應辦事項規定，委託機關認定為核心資通系統時必選。

說明：
1. 依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級以上。
2. 圖示：●-建議辦理，◎-經機關評估個案有必要辦理時，▲-依委託機關資通安全責任等級辦理，導入方式應依機關要求及個案需求辦理，得納入本案或另於他案採購(經確認納入他案辦理者，本案免辦)。
3. 中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

	機關提供ISO 27701或同級規範要求，廠商協助系統符合機關ISO 27701制度或同級規範	●	●	●	提供服務項目涉及個資時應納入要求。
應用程式安全	程式來源不得為來自大陸或港澳地區	●	●	●	若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位部)核定，產品未汰換前，並應加強相關資安強化措施
	廠商提供之應用程式不能有植入後門或木馬程程式	●	●	●	
	於更新程式時提供軟體物料清單 (Software Bill of Materials, SBOM)及安全測試報告，並於每季提供軟體物料清單及安全測試報告	●	●	◎	
存取控制	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準存取控制控制措施，包含帳號管理、採最小權限原則及遠端存取	●	●	●	
	須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制	●	●	◎	
事件日誌保存與可歸責性	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準事件日誌保存與可歸責性控制措施，應建立日誌保存，包含記錄事件、日誌記錄內容、日誌儲存容量、日誌處理失效之回應、時戳及校時、日誌資訊之保護	●	●	●	
營運持續計畫	依據系統防護需求分級，本系統為_____級，需依據_____級系統制定系統營運持續計畫控制措施，包含系統備份及系統備援	●	●	●	
身分識別與鑑別	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準識別與鑑別控制措施，包含內部使用者識別與鑑別、身分驗證管理、鑑別資訊回饋、加密模組鑑別及非內部使用者之識別與鑑別	●	●	●	有關帳號安全如：密碼複雜度、多因子認證等原則，可參考資通安全責任等級分級辦法(附表十，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304)
系統與服務獲得	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與服務獲得控制措施，包含系統發展生命週期需求階段、設計階段、開發階段、測試階段、部署與維運階段、委外階段、獲得程序及系統文件	●	●	●	

各類資訊(服務)採購(含)通性資通安全基本要求參考一覽表

112年9月25日

應用軟體或系統開發服務	資通安全項目	系統與通訊保護	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與通訊保護控制措施，包含傳輸之機密性與完整性及資料儲存之安全	●	●	●	
			資料庫存取及管理操作資料庫之稽核軌跡紀錄，至少包含使用者ID、存取時間、存取之資料庫物件及執行的完整指令	◎	◎	◎	
		系統與資訊完整性	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與資訊完整性控制措施，包含漏洞修復、資通系統監控及軟體、資訊完整性	●	●	●	
			廠商應整體考慮實體、軟體與資料安全，及系統運作的正確性，相關流程應規劃妥適的安全性協定(如TLS保密協定等)，以完整的保護資料不被盜取、竄改，並杜絕發生系統入侵之事件	◎	◎	◎	
		與其他平台系統API介接	其他平台系統介接之網路連線間資料通訊應加密	●	●	◎	
			不得使用管理人員帳號介接資料庫，應另行建立最小(必要)權限的帳號提供應用程式介接資料庫使用	●	●	◎	
			機敏資料的新增、刪除、修改及讀取，應有稽核紀錄	●	●	◎	
			應用系統之資料匯出或介接其它系統，如有去識別化之需求，廠商應配合本機關要求處理	●	●	◎	
		資安防護建置持續監控	資安監控(SOC)機制，廠商須提供 7x24小時全天候監控	▲	▲	▲	
			須提供資安事件應變服務(Emergency Response Service)/IR	▲	▲	▲	
			DDoS 防護服務	▲	▲	▲	
			導入端點偵測與回應機制(Endpoint Detection and Respons, EDR)	▲	▲	▲	
			協助機關就委託案範圍內導入資安弱點通報機制(Vulnerability Alert and Notification System,VANS)	▲	▲	▲	
			導入政府組態基準(Government Configuration Baseline,GCB)	▲	▲	▲	如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。
			導入防毒軟體	▲	▲	▲	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

			導入網路防火牆	▲	▲	▲	
			導入入侵偵測及防禦機制	▲	▲	▲	
			導入應用程式防火牆	▲	▲	▲	
			導入進階持續性威脅攻擊防禦措施	▲	▲	▲	
			導入網路流量全時側錄分析	◎	◎	◎	
		資安維運服務	專案建置範圍之系統軟體或硬體設備，發現之安全漏洞，定期完成更新、修補或進行緊急之應變	●	●	●	
		資安演練	分散式阻斷服務(Distributed Denial of Service,DDoS)攻防演練	◎	◎	◎	涉及重要對外服務之系統建議評估辦理。
			入侵與攻擊模擬 (Breach and Attack Simulation)演練	◎	◎	◎	涉及關鍵資訊基礎設施之系統建議評估辦理
			紅/藍隊演練	◎	◎	◎	
		資安檢測	原始碼檢測	●	◎	◎	核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測。
			程式應用軟體或系統上線前主機弱點掃描	●	●	●	
			程式應用軟體或系統上線前網站弱點掃描	●	●	●	
			程式應用軟體或系統上線前滲透測試掃描	●	◎	◎	
			主機弱點掃描	▲	▲	▲	
			網站弱點掃描	▲	▲	▲	
			滲透測試掃描	▲	▲	▲	
			資安健診	▲	▲	▲	
			取得行動應用 App 基本資安標章	●	●	◎	
			外部攻擊面管理(External Attack Surface Management,EASM)檢測	◎	◎	◎	
		資安治理成熟度評	由專業顧問協助完成標案資安治理成熟度評估	◎	◎	◎	
		資安專責人員	廠商提供資安駐點人員	◎	◎	◎	
		資安教育訓練	提供機關資安及資訊人員 12小時以上	◎	◎	◎	
			提供機關一般人員與主管3小時	●	●	●	
			提供機關資安專責人員取得專業證照	◎	◎	◎	
			廠商需參加機關資安規範教育訓練	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

既有系統功能後續擴充							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級以上。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時，▲-依委託機關資通安全責任等級辦理，導入方式應依機關要求及個案需求辦理，得納入本案或另於他案採購(經確認納入他案辦理者，本案免辦)。 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
既有系統功能後續擴充	資通安全項目	提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	◎	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			導入安全軟體發展生命週期(Secure Software Development Life Cycle,SSDLC)	◎	◎	◎	提請機關資安長確認廠商所開發之系統是否有導入必要。
			不得為大陸地區廠商或第三地區含陸資成分廠商	◎	◎	◎	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		符合國際標準規範	協助系統導入及取得CNS27001及ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準驗證	◎	◎	◎	依資通安全責任等級分級辦法附表一至六應辦事項規定，委託機關認定為核心資通系統時必選。
			機關提供IEC 62443規範要求，廠商符合機關IEC 62443規範	◎	◎	◎	
			機關提供ISO 27701或同級規範要求，廠商符合機關ISO 27701或同級規範	◎	◎	◎	
		程式碼安全	程式來源不得為來自大陸或港澳地區	●	●	●	若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位部)核定，產品未汰換前，並應加強相關資安強化措施

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

			廠商提供之應用程式不能有植入後門或木馬程程式	●	●	●	
			於更新程式時提供軟體物料清單 (Software Bill of Materials, SBOM)及安全測試報告，並於每季提供軟體物料清單及安全測試報告	●	●	◎	
		第三方檢測	原始碼檢測	●	◎	◎	核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測。
			程式功能上線前主機弱點掃描	●	●	●	
			程式功能上線前網站弱點掃描	●	●	●	
			程式功能上線前滲透測試掃描	●	◎	◎	
			主機弱點掃描	▲	▲	▲	
			網站弱點掃描	▲	▲	▲	
			滲透測試掃描	▲	▲	▲	
		資安教育訓練	廠商需參加機關資安規範教育訓練	●	●	●	

各類(含部份服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

應用軟體或系統維運服務							
類型		項目	子項	資料或系統類型			說明： 1.依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級以上。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時，▲-依委託機關資通安全責任等級辦理，導入方式應依機關要求及個案需求辦理，得納入本案或另於他案採購(經確認納入他案辦理者，本案免辦)。 3.中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
				高	中	普	
應用軟體或系統維運服務	資通安全項目	提供服務商	不得為大陸地區廠商或第三地區含陸資成分廠商	◎	◎	◎	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
		符合機關資安政策	機關提供資安規範要求，廠商須符合機關資訊安全要求規範 1.政府機關：資通安全管理法含子法 2.關鍵基礎設施機關：國家關鍵基礎設施安全防護指導綱要、關鍵資訊基礎設施資安防護建議 3.金融機構：參照金融監督管理委員會針對銀行、壽險、產險、證券、期貨、保險經紀人、保險代理人相關資安規範 4.教育單位：教育部資通安全管理實施要點、教育體系資通安全責任等級分級作業規定(草案)、教育體系資通安全暨個人資料管理規範、教育部所屬機關及各級公私立學校資通安全工作事項、國立大專校院資通安全維護作業指引、教育部所管特定非公務機關資通安全管理作業辦法 5.醫療院所：基層醫療院所資安防護參考指引	●	●	●	

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

		應用程式安全	於更新程式時提供軟體物料清單 (Software Bill of Materials,SBOM)及安全測試報告，並於每季提供軟體物料清單及安全測試報告	●	●	◎	
		資安檢測	主機弱點掃描	▲	▲	▲	
			網站弱點掃描	▲	▲	▲	
			滲透測試掃描	▲	▲	▲	
			資安健診	▲	▲	▲	

政府資訊服務採購作業指引

112 年 9 月 25 日

一、預算編列

（一） 按比例編列資安預算並單獨列項：

1. 依「六大核心戰略產業推動方案」項下「資安卓越產業」之推動策略，各機關所提中長程計畫，應依其資訊建設經費編列一定比率之資安經費。
2. 機關辦理資訊服務採購，應依實際需求估算資安經費額度，並單獨計列，並依數位發展部(下簡稱數位部)「資通系統籌獲各階段資安強化措施」之要求達一定經費比例；如因實務作業無法達成上開要求，應敘明原因及擬採行之資安作為。

（二） 必要時先行辦理系統整體規劃：

建置新系統或系統重大變更時，應評估先行編列預算辦理系統整體規劃及資安規劃之必要性，依三層式(資料底層、應用層、使用者介面層)資訊系統開發架構，自行或委託廠商規劃系統架構、分析功能需求、開發資料底層等前置工作，並納入安全系統開發生命周期(SSDLC)規劃，後續再另案委託其他廠商辦理應用層及使用者介面開發。

（三） 依個案特性編列預備費、物價調整費及檢測費：

為因應系統開發過程可能發生之需求新增或變動而衍生必要費用，機關得預估可能所需之額外人月數，編列預備費，未來履約階段於該費用額度內，依實際使用數量結算給付；另考量相關資訊系統開發於履約及驗收時，機關要求廠商辦理檢測，應預估檢測所需費用，編列檢測費，依契約給付檢測費。如屬逾1年之長期服務契約，機關得於契約載明每年服務費用因應物價(如：軟體授權費用)或薪資指數調整之計算方式。

（四） 依法得洽廠商提供意見：

機關應就廠商履約工作內容、各類履約人員成本（得參考行政院主計總處薪情平臺、勞動部職類別薪資資料、政府電子採購網資訊人員薪資資料等）、軟體維護、軟體授權費等項目，並參酌市場行情（包含國際市場）、物價水準等核實編列預算；編列後得依政府採購法（下稱採購法）第34條第1項但書規定，於政府電子採購網公開向廠商說明，並請廠商提供意見及參考資料。

二、廠商資格

（一） 評估是否允許陸資廠商參與：

機關應妥適訂定相應之投標廠商資格，如涉及國家安全或資通安全之採購，機關應於招標文件規定不允許陸資廠商(含其分包廠商)及陸籍人士參與;陸資廠商包含大陸地區廠商、第三地區陸資廠商及在臺陸資廠商。請參閱行政院公共工程委員會(下簡稱工程會)107 年 12 月 20 日工程企字第1070050131 號函。

（二） 必要時限制廠商資金來源比例：

依「機關辦理涉及國家安全採購之廠商資格限制條件及審查作業辦法」，機關辦理涉及國家安全之採購，得依採購案件之特性及實際需要擇定廠商資格限制條件。例如：對廠商資金來源比例有特定限制者，應要求廠商提出廠商董監事、股東名冊、資金來源文件，如涉及僑外資者，應要求廠商提出授權查核同意文件，必要時洽目的事業主管機關協助查察。

三、需求文件

（一） 詳列機關招標需求：

資通系統或軟體開發前，應依個案性質於招標文件載明服務之項目及工作範圍，以明確描述系統需求；機關如能力或人

力不足無法完成者，可委託專業廠商先行辦理系統整體規劃。請參閱工程會111年9月22日工程資字第1111500157號函檢送之「資訊服務採購需求確認之對策與作法」。

（二） 載明服務水準及資安要求：

1. 於招標文件中載明服務水準及品質需求，例如：正常運作時間百分比、運作資源消耗、修復時間、系統反應時間、錯誤率、系統與通訊保護完整性等資通系統防護控制措施、跨平台/跨瀏覽器支援程度、使用者感受等，依據個案的採購類型及需求妥適選擇必要項目，並於招標文件載明，以利廠商合理估價及遵循。(如附件)
2. 機關應依資通安全管理法相關規定、數位部相關規範與政策要求，及資通安全責任等級分級辦法第 11 條第 2 項：「各機關自行或委外開發之資通系統應依該辦法附表九所定資通系統防護需求分級原則完成資通系統分級……」擇定資通系統防護需求(高、中、普)，並依「附表十、資通系統防護基準」及「各類資訊(服務)採購共通性資通安全基本要求參考一覽表」擇定涉及資安之履約項目，於招標文件中載明；資訊財物採購亦得參考上開一覽表擇定須符合之資安項目。

（三） 使用政府資料傳輸平臺及納入零信任架構：

1. 數位部以政府骨幹網路（GSN）為基礎，已建置跨機關資料傳輸專屬通道（T-Road）管理平臺。若資通安全責任等級 A 級公務機關其履約標的涉跨機關資訊傳輸，應評估透過上級主管機關介接或自行介接 T-Road 通道，由資料需求機關依規定向資料提供機關提出申請。經資料提供機關依權責核准後，依 OAS 標準格式進行資料提供，資料需求機關之管理責任應符「政府資料傳輸平臺管理規範」之規定。
2. 為推動國家資通安全政策，發展零信任網路資安防護環境，資通安全責任等級 A 級公務機關應依數位部規劃進程導入零信任架構，以完善政府網際服務網防禦深廣度。

（四） 要求廠商投標時載明執行規劃：

機關於招標時，依機關委託資訊服務廠商評選及計費辦法第5條第8款，依招標文件要求投標廠商提出資訊服務建議書之內容，應包括請廠商載明執行規劃方式，例如：需求訪談、系統分析、系統設計、開發、測試作法及預計時程等，並於開標後審視及評估廠商是否確實了解及符合機關需要。

（五） 妥適訂定招標文件所載之主要部分：

依採購法第 65 條第 1 項、第 2 項規定，採購契約載明應由得標廠商自行履行之全部或主要部分，不得轉包(由其他廠商代為履行)。因資訊服務採購涉及多項專業分工，部分特定服務依市場慣例有分包予其他專業廠商辦理之必要時，機關於訂定招標文件主要部分時應妥為考量，不宜逕明列所有工作項目均為主要部分。

四、 招、決標作業

（一） 載明固定價格決標者議價時不議減價格：

依採購法第52條第2項規定，公告金額以上資訊服務採購以不訂底價最有利標為原則，請機關於招標文件明定以固定費用決標，不議減價格。請參閱工程會112年5月16日工程企字第11200030081號函及「最有利標作業手冊」。

（二） 評選項目考量廠商資安實績及作為：

1. 就涉及廠商過去履約績效之評選項目，將廠商內部資安政策、資安人力配置、曾獲得之認證與獎項等納入評選考量；另為保障採購標的及履約過程之資通安全，應將「投標廠商資安作為」納入採購評選項目，且有一定比率之配分(如：10%，依採購個案中資通系統或服務占比合理考量)，如屬依政府採購法規定無須辦理評選之採購或採其他執行方式者，應以適當方式檢視受託者之資安作為。
2. 依數位部「資通系統籌獲各階段資安強化措施」，資訊服務

採購標的如涉及機關核心資通系統，採準用最有利標方式辦理者，評選委員應包含至少1位資安專業人員；如非採準用最有利標方式辦理者，機關辦理資通系統籌獲案之團隊應至少包含1位資安專業人員，以擇定具資安能力之廠商。

（三） 評選項目不得列「回饋」項目：

為提升採購效益及評選廠商服務之差異，評選項目得列「創意」項目，但不得列「回饋」項目。於採購評選委員會辦理評選時，亦不得於答詢過程中要求廠商提供機關優惠回饋。經採購評選委員會依招標文件規定評選出優勝廠商，即代表該廠商投標文件內容已被接受，不應再強制要求廠商修正。

五、 契約執行

（一） 依契約約定內容協助履約及落實管理：

履約項目如涉及機關既有資通系統之修改或資料介接，機關應善盡定作人之協作義務，提供必要之原始碼或協助廠商間之協調；另亦應落實要求廠商依約履行義務並交付成果(包含原始碼)。

（二） 強化履約使用產品及履約人員之管理：

履約標的或執行過程不得提供或使用大陸廠牌之資通訊產品，履約人員不得為大陸籍人員，若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位部)核定，產品未汰換前，並應加強相關資安強化措施；請參閱行政院秘書長109年12月18日院臺護長字第1090201804A號函及行政院112年6月20日院授數資安字第1121000202號函。

（三） 反覆檢視需求訪談結果，確認後始進行開發：

為深化及細化需求，辦理需求訪談時應反覆檢視及要求廠商展示(例如：示意圖、流程圖或雛型等)，確認符合需要再允

許廠商進行程式開發。

（四） 開發過程設定查核點，反覆檢視執行成果：

契約應依系統開發各階段載明查核點，反覆檢視執行成果並要求廠商展示(如開發畫面、資料庫架構、使用流程、功能測試、整合測試等)，並定期(開會)追蹤檢討，查核時間不列入工期計算；如經查核有不符合契約約定及機關需要者，應即要求廠商配合改善，非可歸責於廠商者，應依查核狀態調整履約期間。

（五） 機關新增需求應合理增加經費及期程：

履約過程如確屬機關需求改變或增加情形，應辦理契約變更，給予必要之履約期間與費用。

（六） 機關以取得授權利用為原則：

基於尊重著作人創作、成果能善加運用開發與鼓勵廠商參與政府採購之意願，機關與廠商約定履約標的著作權歸屬時，應考量機關與廠商間之平衡，先評估原始碼無洩漏或被竊取不當使用之風險，並依風險採取必要措施。另為利後續系統維護管理及功能增修，機關應儘量以取得著作財產權之授權利用為優先，包括轉授權或再製權等。

（七） 履約及驗收得請具資訊、資安專業人員協助確認：

為確認廠商履約過程及成果符合產業實務且滿足機關需求，得邀請具資訊專業之專家學者協助確認；如履約內容涉及機關之核心資通系統，並應優先考量聘請外部資安專家為顧問或委員，協助機關檢視相關資安管理作為。

六、 爭議處理

（一） 善用契約雙方約定之處理機制：

現行工程會提供之「資訊服務採購契約範本」第 19 條已載明多元之爭議處理方式，機關可善用爭議處理小組機制，並選擇具有資訊、資安專業之專家學者擔任小組委員，協助協

調爭議。

（二） 機關成立採購工作及審查小組提供意見：

依採購法第 11 條之 1，機關辦理資訊服務採購得依採購特性及實際需要成立採購工作及審查小組，協助審查採購需求與經費、採購策略、招標文件等事項，及提供與採購有關事務之諮詢，開會時並得邀請具資訊、資安專業之專家學者列席，協助審查及提供諮詢。

附件　常用資訊服務等級協議(SLA)之參考項目

服務等級協議(SLA)係衡量服務可用性、可靠性、安全性等指標，常用SLA性能指標如下，機關可依個別系統之類型、重要性、複雜性、機敏性及使用情境選用項目：

一、 系統及服務可用性

(一)環境面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V	V	V	服務韌性:電力、水、網路、空調、濕度調節之備援與調節方式，確保系統正常運作於發生異常時有足夠之應變緩衝時間。		0
		V	V	Ÿ對外網路環境：骨幹網路、交換器、路由器異常故障，造成連線與服務中斷，其累計時間每月不得超過____小時(約為____%可用率)。		0
(二)服務面						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V	V	V	服務可用性(Service Availability)：該指標衡量服務對用戶可用的時間百分比，其計算應考慮到其他須排除之因素，如計畫中維護和升級；例如，SLA 可能規定該服務必須 99.9%的時間可用。(計算公式： 服務可用性 =（本月總小時數-停機時間）/ 本月總小時數 × 100%)	0	
V	V	V	V	正常運行時間百分比(Uptime percentage)：正常運行時間通常按每個日曆月或結算週期進行追蹤及報告。	0	
		V	V	平均故障間隔時間（Mean Time between Failure, MTBF）：服務故障之間的平均時間。	0	
		V	V	平均修復時間（Mean Time to Recovery, MTTR）：恢復服務故障的平均時間。	0	
			V	系統穩定度：每月每項服務中斷次數之累計不超過次數。	0	
	V	V	V	反應時間：使用者在端末設備輸入應用系統所需資料，自按功能鍵至應用系統將處理結果傳回作業端止的時間，其作業量之____%系統反應時間應在____秒內。	0	
	V	V	V	批次作業時間：自該批次作業工作啟動至作業完成之時間應於____小時內完成____筆資料。	0	
	V	V	V	檔案傳輸時間:在工作天之作業時間(上午 8 時	0	

				~下午 5 時)內，傳送____GB 檔案應於____分鐘內完成。		
			V	滿意度調查：定期對終端使用者就系統使用上，調查滿意度評分，每次調查應不低於____分。		0
(三)永續維運與管理						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V	V	V	營運異地備份/備援：備份數、儲存媒體種類、異地備份數等，以及備份還原測試頻率、備援演練次數。		0
		V	V	系統備份/備援恢復作業時間 (RTO):每次操作系統備份/備援回復作業應於____(時間)內完成。		0
		V	V	資料回復可接受之時間點(RPO):可允許的最回溯落差____(時間)。		0
		V	V	最大可忍受中斷時間(MTPD)：最大可忍受系統中斷服務____小時。		0
		V	V	備品供應:涉及硬體提供者，廠商應至少準備____(例如 1/3)之備品，以利於故障時及時更換。		0
		V	V	Ÿ 網路、資安、資料庫或伺服器等設備若具備高可用性(HA)架構，需依合約規範的時間頻率，執行本地端的 HA 切換演練，確保設備切換可於時限內正常使用，每月至少切換測試一次，未能成功者計罰____元，且應於____日內再測試，直至成功為止。		0
(四)資通安全品質：						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V	V	V	風險評鑑與風險管理計畫：依照政府資安等級規定進行風險評鑑並依評鑑結果訂定風險管理計畫。	0	
		V	V	實體及遠端登錄管制與稽核:避免帳號洩漏或破解致影響系統安全與正常運作，應有效管控並定期稽核有無不允許或異常的登錄情形。	0	
			V	漏洞修補:避免因疏漏造成整體服務暴露於風險之中，廠商應就所提供服務涉及之軟硬體、作業系統及開發之程式，定期檢查更新並予掃描、測試及調整，確保整體運作穩定、高效及安全。當接獲弱點通報時，應即時完成修補；於完成修補前，應規劃緩解措施及管理作為，加強監控。	0	

			V	資通安全政策執行品質:分別計算每月及每季未依機關或契約資通安全規定執行之次數。	0	
			V	資安測試之改善：定期執行資安測試，包括安全通訊協定、系統弱點掃描、應用程式弱點掃描、App 資安檢測等，其有需改善者而未能於契約約定期限內改善完成者，每月/不得超過____%。	0	
			V	安全防護計畫執行：定期檢視監控資安日誌如防火牆、入侵偵測系統、應用程式防火牆、安全資訊與管理系統等並訂定防護計畫與措施，每季未能執行次數不得超過____次。	0	
			V	資安事件之通報及應變：自知悉或接獲資通安全事件通知或即時警示後，應至遲於____分鐘內通報機關，並於____小時內提供資通安全事件等級評估、處理應變規劃及建議。	0	
			V	調查及處理資安事件之時效：資安事件發生後需依照合約規範的時限內的完成損害控制或復原作業，並於____日內送交調查、處理及改善報告（或協助機關調查處理）。	0	
			V	外部稽核：廠商需配合機關進行_____(如：ISO 27001、ISO 20000，機關視需要載明)國際資安認證外部稽核驗證，其每次稽核所列缺失不得超過____項。	0	

二、 廠商之服務品質

（一） 設計與開發階段:						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
	V	V		未依機關同意之流程或設計準則開發之比率:除屬機關需求變更者外，廠商疏漏或未依機關確認之內容進行開發之比率，可依展示次數逐步降低，提升系統完善及整體性。	0	
	V	V		未依限回應問題之次數：可依不同階段及態樣規範機關所詢問題之回應時間。	0	
(二)測試驗證階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
		V		單元測試流程通過比率:在單元測試(驗證程式碼的每個獨立部分是否正常運作)中，通過測試的數量與總測試數量的比率應達____%以上。	0	
		V		整合測試通過比率：在整合測試(驗證程式碼的各個部分是否能夠正確地協同工作)中，通過測試的數量與總測試數量的比率應達____%以上。	0	
		V		效能調教次數：廠商應於____次內調教效能，	0	

				達成契約約定之具體的績效基準(Specific performance benchmarks)。		
(三)上線前準備階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
		v		壓力測試：系統能同時、瞬時支援使用人數的上限，系統上線前應模擬正式使用(尖離峰、歷史事件等)環境進行壓力測試。	0	
		v		資料移轉時間及正確率：可分階段訂定，移轉時間應每次縮短；資料漏失或錯誤率應逐次下降，且同一資料錯誤情形不得超過____次。	0	
		v	v	上線演練作業之次數與所需時間:可分次訂定，切換所需時間應每次縮短；超過機關指定之時間應紀錄為失敗(可分模組或功能計算)，上線前成功比率應逐步提升。	0	
		v	v	客服準備情形:依機關同意之問答內容進行抽測與實作，抽測通過比率應達____%以上。	0	
		v	v	人員之教育訓練：經協助受訓人員完成機關指定之測試項目應達____%；受訓人員滿意度應達__%(前開比率可分階段調高)。未能達成前開比率者，廠商應再辦理一次，仍未達成者，按差距部分每____%計罰____元。	0	
(四)建置及維運階段						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
			v	事故發生通報時間：異常事件發生時，廠商應於____(時間)內通知機關聯絡窗口。	0	
			v	廠商反應時間(Service provider response time)：廠商應於____(時間)內回應使用者問題或請求。	0	
			v	解決時間(Resolution time)：場商記錄問題後應於____(時間)內解決問題。	0	
			v	錯誤率(Error rate)：在____(時間)內，資訊系統服務中出現錯誤的次數與總次數的比率。錯誤可以是系統錯誤、應用程式錯誤、網路錯誤等。	0	
			v	軟硬體設備修復時限：軟硬體設備發生異常時，廠商於知悉或機關通知後應於____(時間)內到達現場，於____(時間)內內修復；若無法於時限內修復，應無償提供同等(含)以上替代品供使用。		0
			v	舊系統資料儲存：新系統上線後，舊系統資料應儲存於可存取環境並保留____月/年。		0
			v	軟硬體設備維修妥善率：任一設備於一定期間內連續發生____次異常問題至需更換或維修者，視為未達妥善率要求。		0

(五)其他						
規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V	V	V	交付文件及品質:廠商按照契約規範交付非屬履約成果之文件者(如工作日誌、每周報告)，因內容缺漏、不足及錯誤至退件之次數，每件不得超過____次。	0	
V	V	V	V	召開履約關理相關會議：未依契約約定召開會議者，每季不得超過____次。契約約定之廠商人員未出席會議次數，每季不得超過____次。	0	
V	V	V	V	服務團隊成員要求：廠商提供服務團隊成員資格、證照與人數要求，每季更新統計，若低於契約要求之____%者(如 95%)，依差異之每____%計罰____元。	0	

三、 使用者體驗

規劃	設計	建置	維運	常用服務水準項目	軟體	硬體
V	V			跨瀏覽器支援：使用者端網頁介面須支援之瀏覽器類型，如：Microsoft Edge、Google Chrome、Firefox、Apple Safari。	0	
V	V			行動裝置支援：使用者端網頁介面須支援之跨平台行動裝置，如：適用 Android、iOS 作業系統。	0	
V	V			響應式網頁設計(Responsive Web Design；RWD)：讓使用者能夠在各種不同尺寸或解析度的裝置上都能夠輕鬆地瀏覽、使用網站，而不需要因為裝置不同而產生閱讀體驗上的問題。	0	
V	V			通過無障礙標章認證。	0	
	V			使用者填寫資料：使用者建立資料時，每頁面填寫平均時間應在____分鐘內。	0	
	V			提供友善列印、字體大小調整、暗色等模式供使用者選擇。	0	