附件5 「雲端服務商提供資訊系統部署、託管及維運服務」RFP 資安需求範例

本文件公告前為密級資料，敬請妥善保管

○○年度

「◯◯雲端資訊系統建置、託管及維運服務案」計畫

建議書徵求說明書

○○○○○○

中華民國○○ 年○ 月

目　次

1. 專案概述

1.1. 專案名稱

本專案名稱為「○○雲端資訊系統建置、託管與維運服務案」(以下簡稱本專案)

1.2. 專案目標

- 提供具備隨需隨用、網路連接、資源共享、快速彈性即可測量服務的雲端服務平台。
- 建立符合本機關網路、系統、資料安全目標，以及有效存取控管、營運持續、事件通報與蒐證稽核之安全管理機制。
- 達成本專案服務水準需求。

1.3. 專案範圍

(依各機關專案需求撰述專案範圍)

1.4. 專案時程

(依各機關專案需求撰述專案時程)

2. 系統環境現況說明

(依各機關專案撰述現行資產、設備、網路及系統環境，以及在不揭露系統重要敏感資訊之前提下，簡要說明納入本專案雲端服務資訊系統之資產清冊及安全等級評估情形，俾利廠商據以規劃相關控制措施)

3. 專案建置需求

3.1. 專案整體需求

(依各機關專案需求界定服務模式為 IaaS、PaaS 或 SaaS 之公有雲)

3.2. 投標廠商資格限制

- 廠商不得為大陸地區廠商第三地區含陸資成分廠商。
- 分包廠商亦不得為大陸地區廠商第三地區含陸資成分廠商。
- 未經本機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區或其指定排除之國家。
- 本專案廠商宜通過專業之認證，如 ISO 27001 及 CNS 27001 等。

3.3. 資源需求

3.3.1. 系統資源需求說明

(依政府機關專案需求敘述雲端資訊系統之數量、配置、規劃、運作、管理及架構等)

3.3.2. 使用者資源需求

(依政府機關專案需求說明雲端資訊系統之使用者、系統管理者、資源分配者等各種角色責任分工及人數等)

3.4. 安全需求

3.4.1. 整體安全需求說明

對於專案內各項資訊系統，投標廠商應依政府「資通安全責任等級分級辦法(草案)」及機關所認定之資訊系統安全等級，採行適當安全控制措施，以確保資訊系統達到應具備之安全防護水準。

廠商應針對納入本專案之資訊系統安全等級，依據政府「資通安全責任等級分級辦法(草案)」所需採行之控制措施，於評選階段提出自我說明報告或由第三方公正單位提出驗證報告，以確認執行情形。

廠商應通過國際資訊安全管理標準 ISO 27001 驗證之證明文件，於投標時應於有效期內，且認證地點應與本案營運所在同一地點。

廠商須將電腦處理私人事務與機關事務分開使用，以降低資料外洩的風險。私人事務包括 Email、電話、線上論壇、傳真、即時通訊等。

註 1：以下參照指引第 2.5.4 雲端委外風險與注意事項乙節，說明在不同雲端服務模式下，廠商應負責部分：

服務模式 / 安全管理	IaaS	PaaS	SaaS
可用性管理	以服務水準協議方式，要求廠商確保虛擬主機平台，包含以下之伺服器、儲存及網路等軟硬體設施之可用性，並檢視廠商營運持續、資料復原計畫及執行情形。其中營運持續之異地備援距離本地至少 35 公里(含)以上，且當一台實體伺服器故障可於 10 分鐘內將其上 VM(Virtual Machine)移轉至其它實體主機中重新開啟。	1.達成 IaaS 可用性管理。 2.確保雲端應用系統平台，如資料庫、儲存空間等可用性。	1.達成 PaaS 可用性管理。 2.確保雲端軟體服務之可用性。

服務模式 安全管理	IaaS	PaaS	SaaS
存取控制	依資安規範要求廠商建立虛擬主機平台暨所屬軟硬體設施存取控制機制，包括帳號安全認證、權限管理、網路安全傳輸及遠端存取控管，並能驗證其有效性。	除將帳號安全認證管理提升至雲端應用系統平台層次外，並達成 IaaS 其餘存取控制措施。	除將帳號安全認證管理提升至雲端軟體服務層次外，並達成 PaaS 其餘存取控制措施。
弱點管理	要求廠商確保虛擬主機平台暨相關軟硬體弱點皆能有效管理與更新。	1.達成 IaaS 弱點管理。 2.確保雲端應用系統平台弱點皆能有效管理更新。	1.達成 PaaS 弱點管理。 2.確保雲端軟體服務弱點有效管理更新。
變更管理	要求廠商對於虛擬主機平台暨相關軟硬體皆有變更標準、規範與程序。	1.達成 IaaS 變更管理。 2.確保雲端應用系統平台落實變更管理。	1.達成 IaaS 變更管理。 2.確保雲端服務平台落實變更管理。
設定管理	依資安規範要求廠商對於虛擬主機平台暨所屬軟硬體進行適當配置與設定，以強化其安全性，並檢視廠商定期測試評估情形。	1.達成 IaaS 設定安全管理。 2.確保雲端應用系統平台設定安全管理。	1.達成 PaaS 設定安全管理。 2.確保雲端軟體服務設定安全管理。
意外應變	對於虛擬主機平台暨所屬軟硬體應有事件應變處理機制，包括管理政策、規範、程序及	同 IaaS，並包括雲端應用系統平台部分。	同 PaaS，並包括雲端軟體服務部分。

服務模式 安全管理	IaaS	PaaS	SaaS
	處理窗口，並檢視廠商定期演練情形，確認有效性。		
監測系統使用與存取	廠商對於虛擬主機平台之設定、使用情形、控制措施及重大改變事件，應提供可靠、持續性的監控機制。	同 IaaS，並包括雲端應用系統平台部分。	同 PaaS，並包括雲端軟體服務部分。
資料安全	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，避免遭竊或有不當侵害情形發生。	1.達成 IaaS 資料安全管理。 2.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。	1.達成 PaaS 資料安全管理。 2.雲端軟體服務內如有機密或個人資料應依相關法令強化資料安全防護措施。
電子蒐證	廠商對於虛擬主機平台應能建立電子蒐證機制，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、虛擬主機異動、資料存取及重要安全性事件等，並應確保其完整與正確性。	1.達成 IaaS 電子蒐證標準並擴展至雲端應用系統平台層次。 2.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落實電子蒐證機制。	1.達成 PaaS 電子蒐證標準並擴展至雲端軟體服務層次。 2.雲端軟體服務內如存有機密或個人資料應依相關法令落實電子蒐證機制。
實體環境	設備所在建築物須符合 921 地震後內政部公布之建築法規標準，5 級抗震設計。(提供土木結	達成 IaaS 實體環境管理。	達成 IaaS 實體環境管理。

服務模式 安全管理	IaaS	PaaS	SaaS
	構技師出具之「建築物結構證明書」佐證資料)；門禁系統採 24 小時、365 天實體管制：所有溫度、溼度和門禁監控元件之狀態一律由中央環控系統進行控管；監控錄影應 24 小時無死角，且錄影保存期限至少 30 天。		

本項除界定不同雲端服務模式(IaaS/PaaS/SaaS)廠商應負責安全管理事項，機關實際訂定合約時，應依本身系統環境、需求並在預算許可下，適時調整合約，將相關需求納入要求廠商協助辦理。

註 2：政府機關應檢視系統本身之安全需求並依「資通安全責任等級分級辦法(草案)資通安全責任等級分級辦法」(草案)，將必要之項目控制措施納入合約需求，並可參考經濟部工業局共同供應契約雲端服務採購契約文件，針對自身需求及技術規格部分適時調整。

3.4.2. 網路及系統安全需求

3.4.2.1. 網路安全需求

廠商應提供安全的系統、網路架構、傳輸協定及遠端存取控制，以確保機關資料在雲端系統環境中安全傳輸無虞，廠商應說明實作之傳輸加密機制、強度及相關做法，以防止未授權之資訊揭露或偵測資訊之變更。機關在上傳檔案或透過 Web Service 等機制匯入檔案時，系統應提供安全性防毒檢測

服務，以確保所分享的檔案是安全的，並說明 APT 惡意程式防制方式。

3.4.2.2. 持續性監控

廠商應採用自動化工具針對雲端資訊系統之設定、控制措施及重大改變事件，提供可靠、持續性的監控機制，除確保機關能掌握目前系統使用與運作情形，事件發生時並能迅速掌握處理，廠商於發現系統遭入侵、資料遭竊、竄改或有其他違反個人資料保護相關法規時，應即刻通知本機關並依本專案應變處理機制辦理 。

廠商應說明防止駭客入侵的途徑及惡意流量進行阻擋的網路安全防護、防火牆、入侵偵測系統 IDS(intrusion detection system)、入侵防禦系統 IPS(Intrusion Prevention System)、阻斷服務攻擊 DDoS (Distributed Denial-Of-Service)、惡意 IP、防毒及防止 APT(Advanced Persistent Threat)惡意程式等防護解決方案。

3.4.2.3. 事件緊急應變處理與鑑識需求

廠商應根據日常監控與狀況，主動分析是否屬安全事件，並依照行政院國家資通安全會報相關通報應變標準啟動對應之處理程序，協助本機關執行相關處理程序，如涉及違法個人資料保護法相關法規時，必要時應協助本機關進行後續和解或訴訟程序。

對於本機關發生之重大資安事件，廠商應於 30 分鐘通知機關，提供 7 天 X 24 小時全年無休之緊急應變處理服務，在本機關要求下於規定時限內指派人員進行事件緊急應變協同處理(廠商人員進場、退場時機及報告、產生文件由廠商於服務水準協議書提出)。

本機關判斷須進行緊急應變處理時，廠商需於接獲通報時間起算 6 小時內抵達本機關指定地點，並於事件處理完畢 3 個工作天內，將處理經過作成報告(涵蓋防護提升作法及相關改善建議)交付本機關，廠商對本機關就本項

履約服務辦理下列事項：

- 於接獲通報時間起 24 小時內完成本機關資安事件之初步緊急應變處理。
- 接獲通報時間起 72 小時內完成下列項目：
  - 協助本機關針對網路及系統安全入侵行為進行事件之分析、封鎖、圍堵及根除(含提供相關移除程式)。
  - 提出處理事件過程中所必要之系統備份及復原建議方案。
- 廠商參予本機關執行緊急應變服務時，應配合以下事項：
  - 廠商應於接獲通報時間起算 6 小時內配合本機關成立緊急應變小組協同處理，並隨時提供最新處理資訊。
  - 廠商參與應變處理人員負有保密義務,不得公開散布或傳閱應變過程中所有執行之內容或文件。
  - 緊急應變過程所產出各項文件資料權利歸屬本機關。
- 在不影響數據的完整性及系統運作下，政府機關基於刑事或非刑事的目的，可要求投標廠商或指定第三方針對雲端資訊系統進行數位鑑識，廠商應配合政府機關針對專案內各項設備與系統進行鑑識，並在機關授權下使用數位鑑識工具,如要求廠商進行數位鑑識時,應於接獲本機關通知 30 天內，依數位鑑識標準作業程序完成數位鑑識書面報告交付本機關。(鑒於雲端服務系統之特殊性，政府機關除要求廠商外，並可保留第三方數位鑑識之權利)
- 廠商應於建議書提出數位鑑識團隊成員，具有專業證照、資安事件鑑識經驗及採用工具，同時將數位鑑識管理程序列入作業安全管理計畫內。
- 投標廠商因可歸責之事由逾期未完成改善者，本機關得要求廠商將相關資料返還或刪除雲端資訊系統之任何數據，並逕行終止合約，並自解約之翌

日起依本契約相關條款辦理。

3.4.2.4. 安全認證機制

廠商應能提供良好之帳號管理機制，包括帳號之申請、開通、停用、刪除，以及定期審核程序。對於系統中已逾期、臨時緊急建立或閒置之帳號應刪除或禁用，且應設定帳號閒置或可使用期限，並自動將使用者登出；另應系統帳號違常使用監控機制，並能於發現違常時回報管理者。

對於重要之系統管理者或高度敏感使用者，廠商應提供可使用個人身分驗證設備(如智慧卡或生物辨識設備等)，並符合 HSPD-12 安全標準之雙因認證機制，以確保遠端使用者登入雲端資訊系統時，能有效避免身分遭盜用、篡改或偽造。

廠商對於系統中之使用者通行碼或加密密鑰，必須提供良好的安全管理機制，以確保未經授權之使用者能任意存取並危及雲端資訊系統安全，有效保護雲端資訊系統資料安全。

3.4.3. 隱私安全需求

3.4.3.1. 符合個人資料保護法及相關法規

對於雲端資訊系統中之個人資料數據，廠商必須依據法令辦理相關保護與管理事項，除個人資料檔案之備分保存外，亦應包括個資在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體所衍生之軌跡資料，如資料存取人之代號、存取時間、使用設備代號、網路位址(IP)、經過之網路路徑等，以比對、查證資料存取之適當性。

3.4.3.2. 隱私衝擊分析

為確保個資蒐集、處理及利用過程中，所可能隱含的資訊安全風險，並避免個資使用不當事件發生，廠商每年應至少針對雲端資訊系統中涉及個資部分辦理個人隱私衝擊分析 1 次，並於辦理完成 30 日內提出個人隱私衝擊

分析報告，內容並應包含風險改善措施與建議，其程序並應列入作業安全管理計畫內。

(本項涉及雲端服務之個資整體管理，所需費用及工作項目複雜龐大，可考慮納入其他類似 BS10012 個資服務專案內，並要求廠商依機關隱私衝擊分析報告協助風險改善)

3.4.3.3. 資料儲存

機關利用雲端服務之所屬一切資料存取、備份及備援之實體所在地為我國境內 ，且系統中之機密資訊應進行加密。

3.4.4. 電子蒐證(E-discovery)

3.4.4.1. 雲端電子紀錄蒐集與保護管理

- 為利於日後民刑法訴訟所需並提供足夠的證據力，廠商應針對專案資料內容及政府需求於專案期間內提供電子蒐證機制，蒐集內容與項目由雙方另行議訂，廠商除提供必要空間儲存電子紀錄外，並提供瀏覽、下載機制供政府機關使用。(政府機關除可依「資通安全責任等級分級辦法(草案)資通安全責任等級分級辦法(草案)」，臚列各項安全等級所需之控制措施外，如涉及個資時亦可依相關法令將相關紀錄需求納入合約)
- 在蒐集的過程,應遵守相關法規及標準程序進行,以持續維持正確與完整，確保日後相關證據可被法庭採納。
- 廠商應保留雲端資訊系統紀錄檔，並應防止系統紀錄遭竄改及刪除，另能依使用者區分存取權限，包括設定唯讀狀態與限定僅有特定授權者能存取稽核交易紀錄，另應依機關需求定期備份稽核紀錄到機關指定之系統外安全處所。
- 運用加密機制，以保護稽核資訊之完整性。

3.4.4.2. 電子紀錄之發現與搜索

廠商應提供電子紀錄發現與搜索必要工具，必要時得將所發現與搜索出之資訊納入前項蒐集與管理項目，所增加費用由雙方另行協商。

3.4.5. 漏洞修補及安全建議需求

- 漏洞修補更新需求：投標廠商於本專案所提供各項軟硬體設備，應能達成自動即時更新修補漏洞目標，有效防止漏洞、弱點所造成危害，如相關漏洞、弱點無法自動即時更新，亦應提出替代方案，並說明改善方式及期程經本機關審查通過。
- 資訊安全改善建議：投標廠商應隨時研究與注意最新資訊安全現況，遇有系統或設備原廠重大系統安全漏洞更新發布或外界重大安全事件發生，或接獲修正通知時，應向本機關發布資訊安全改善建議，並協助辦理防護及修正、修補工作。

3.4.6. 資安稽核需求

本機關基於法令及合約需求，得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形，且投標廠商負有配合並提供本機關稽查所需相關文件資料之義務。

3.5. 專案管理

得標廠商應於決標後◯日內提交專案工作計畫書，經本機關審查通過後，做為工作交付項目並為執行專案之依據,內容應包括對本計畫之執行敘述，含專案管理、組織、人力、分工、職掌、計畫工作項目及時程、查核點、建構管理、品質管理、需求異動管理及服務水準協議。

3.5.1. 專案組織與職掌

3.5.1.1. 成立專案小組及分工

- 投標廠商應成立專案小組，其成員包括：專案經理、系統工程師、網路工程師、資安工程師，負責本專案之各項需求規劃、協調、分析、設計、測試及資安維護等工作。
- 本專案參與人員需具資訊安全相關技能，並具有個資隱私與資安專業證照或其他類似之文件。

3.5.1.2. 專案小組成員

- 投標廠商須提供專案小組成員之學經歷、專長、負責本專案之工作項目及內容，並檢附專案小組成員勞、健保等證明文件與資安相關證照。
- 專案小組成員應簽訂保密切結書，必要時得配合接受身家安全調查。
- 專案小組成員不得有非本國籍勞工，若有分包廠商，其成員亦同。

3.5.1.3. 專案經理之資安職責

本專案廠商之專案經理應具備良好之協調及資訊專業能力，以掌控本專案之執行進度及成果，並符合本機關需要。

專案經理應負責與本機關承辦人員相關資安業務之協調，同時應推動、協調及督導下列資訊安全管理事項，包括：資訊安全責任之分配與協調、資安政策與規範的遵循、組織成員資安教育訓練、資訊資產保護事項及資訊安全事件之檢討等。

3.5.1.4. 專案小組成員異動

專案執行期間，專案小組成員如有異動，得標廠商應於二週前(日曆天，含異動當天)函請本機關同意，並檢附接替人員相關學經歷、專長、勞健保等相關證明文件以及保密切結書，經本機關審核通過後更換。

本機關對不符本專案執行需要之人員，得要求得標廠商更換，得標廠商應提供適當人選經本機關審核通過後更換，並於兩週內完成人員交接。

3.5.2. 交付項目與交付日期

(依各機關專案需求撰述交付項目與交付日期)

3.5.3. 建構管理

- 資料管理應包括：紙本資料管理及電子檔資料管理。
- 組態管理應包括：組態項目、建立組態管理環境與組態項目識別方式、組態項目納管與記錄、組態項目版本之建立與發行、已納管組態項目之變更管制、組態管理紀錄留存、組態稽核及基準，廠商應確實執行組態管理，以確保系統之完整性及一致性，以符合機關對系統品質及資訊安全的要求。

3.5.4. 品質管理

除另有規定或經雙方同意外，每月應至少召開專案工作會議 1 次，確實檢討該段期間本專案各項作業進度與目標達成情形、下一段期間預定進度、各方待配合協調應注意及改善事項等事宜，並於會後 3 個工作天內做成會議紀錄，並經本機關審核通過。

本專案各項交付文件內容與產品,應於專案工作會議中提報本機關確認後，再行交付。

得標廠商應依據本專案規定之期限交付工作項目文件與產品，由本機關進行審查作業，審查項目如有不符本專案需求者，得標廠商應於 14 天內完成修正，並提供予本機關複審。

3.5.5. 需求變更管理

請廠商建立需求變更之標準、規範、程序及管理上之建議。。

3.5.6. 服務水準協議

- 效率、可用率及安全性規範，如全年系統各項功能，可正常提供使用者之

時間百分比，不得低於◯◯%。

- 不中斷服務，如機關發現系統故障致不能運作時，得隨時在服務時間內以電話通知廠商維修，廠商接獲通知後，須於 4 小時內修復完畢。
- 滿意度調查，如機關應每季針對廠商之服務成效，針對使用者執行滿意度調查，其滿意度不得低於◯◯。

3.6. 作業安全需求

3.6.1. 作業安全管理計畫

投標廠商應依本專案需求提出作業安全管理計畫，內容包括如下：

3.6.1.1. 服務範圍

主要在描述服務的時程、服務形態、服務範圍、風險要項、人員權責劃分及系統資料成長預測等。

3.6.1.2. 服務驗收或稽核服務之管理程序

3.6.1.3. 專案人員每年應定期參與個資、隱私及資安管理相關教育訓練。

3.6.1.4. 專案人員籌組與異動時之規劃

例如：安全管理、教育訓練及人員安全查核(含僱用前、僱用中、結束僱用或改變職務)。

3.6.2. 服務結束、終止之措施

本合約期滿、終止或解除時，投標廠商應依本機關之指示，將因履行本契約所蒐集之所有資料返還予本機關指定人員，並採用永久有效之方法刪除無法返還之個人資料(包括電磁紀錄、紙本或其他任何形式儲存者)，投標廠商並應提出相關證明文件，內容包括銷毀或交還之項目、數量、時間、方式、簽收人等，同時應以書面切結其並未持有任何因執行本契約而蒐集

之個人資料。

3.6.3. 所有權與智慧財產之保障

- 廠商因履行契約所完成之著作，其著作財產權之全部於著作完成之同時讓與機關，得標廠商放棄行使著作人格權。得標廠商保證對其人員因履行契約所完成之著作，與其人員約定以得標廠商為著作人，享有著作財產權及著作人格權。
- 除另有規定外，得標廠商如在契約使用專利品，或專利性履約方法，或涉及著作權時，其有關之專利及著作權益，概由得標廠商依照有關法令規定處理，其費用亦由乙方負擔。

3.6.4. 遵循適法性做法

- 遵守個資法與各項公務、業務機密保護法規。
- 遵守機關之資安政策與規範。

3.7. 其他需求

3.7.1. 保固服務

得標廠商於保固期間，當系統異常造成運作中斷或部分無法正常運作時，應有備援方案進行系統線路切換，提供機關於主系統服務中斷時的配套方案，並依契約規定，進行異常之排除。

3.7.1.1. 後續服務規劃

投標廠商應提出日後簽訂軟硬體維護契約相關工作內容之說明(本項依契約內容而定)。

4. 交付文件與產品

本專案得標廠商需根據建議書徵求文件、契約及得標廠商所提建議書，經本機關認同之各項工作結果，作為本專案之交付項目，本專案交付之文件與產品其所有權及使用權歸屬本機關所有，另因教育訓練及廠商提供獲得之經驗、文件等本機關可自行運用，日後開發各項新增功能與服務項目，毋須經由得標廠商同意，交付項目至少包含下列各項：

4.1. 設備軟硬體部分

(依各機關需求詳列所交付之軟硬體清冊及軟體授權證明)

4.2. 資安報表文件

- 為了解機關網路安全現況，廠商至少每月提供資安報表服務，並納入每月服務工作報告書內，俾作為機關風險分析及營運決策基礎，報表內容至少包含設備定期維護紀錄、管理維護服務事項及其他與本案相關之履約佐證資料，同時提供必要改善建議與諮詢服務。
- 除定期提供資安報表服務外，在發生資安事件或察覺相關異常警訊時，廠商得應本署要求提供即時報表資料。
- 本項報表服務除書面資料1份外，至少須提供Word或PDF等格式電子檔。

5. 驗收

- 廠商履約所供應或完成之標的，應符合本契約規定，無減少或滅失價值或不適於通常或約定使用之瑕疵，廠商所提供設備必須是符合標準規定的生產廠商所製造且為新品，僅限於西元○○○○年 1 月以後出廠，並應於完成履約期限前交付原廠出廠證明(如有裝備序號者，並同時提交序號清冊)。

- 驗收程序：廠商於維護期間，應於每期完成履約標的維護後，依實際履約情形檢附服務工作報告書，內容包含系統設備維護紀錄、滲透測試服務報告及弱點掃描服務報告等相關資料向本機關報驗，本機關應於接獲廠商通知備驗或可得驗收之程序完成後○日內辦理驗收，並做成驗收紀錄。

- 廠商如提供設備應可於原製造廠(或生產國)官方網站，取得相關功能及技術規格規範等諸元資料，並以市場流通之通用型號設備為主(如非通用型號或係針對本案開發設計之設備，並應於完成履約期限前交付國內、外公證第三者測試認證書)，並須註明交付設備明確型號及設備型錄並於建議書答標項目內容標示，如未註明則以該系列產品最高等級設備交付。

- 廠商不於本專案契約期限內履約(改正)、拒絕履約(改正)或無法履約(改正)者，本機關得採行下列措施之一：

  自行或使第三人履約(改正)，並得向廠商請求償還履約(改正)必要之費用。

  終止或解除契約或減少契約價金。

  因可歸責於廠商之事由，致履約有瑕疵者，本署除依前二項規定辦理外，並得請求損害賠償。廠商依契約規定所負之損害賠償責任，僅限於直接損失，並不包括其他任何間接性或衍生性之損失。

6. 建議書製作規定

(依各機關專案需求撰述專案範圍)

7. 評選辦法

(依各機關專案需求撰述專案範圍)

7.1. 投標廠商限制

- 廠商不得為大陸地區廠商第三地區含陸資成分廠商。
- 分包廠商亦不得為大陸地區廠商第三地區含陸資成分廠商。
- 本專案禁止移至本國地區以外國家與地區開發。
- 本專案參加成員禁止非本國國民參加。

7.2. 終止評選規定

本機關得因故終止評選事宜，通知投標廠商領回建議書。

7.3. 未盡事宜

本專案依據依行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、機關委託資訊服務廠商評選及計費辦法等及相關法規規定辦理。