**臺灣基督教門諾會醫療財團法人**

Mennonite Christian Hospital

**網路微切分管理系統建置-徵求建議書說明文件**

Request For Proposal

2025/03/11

**內容目錄**

目錄

* [1. 專案描述 2](#_Toc192861515)
* [2. 現況說明 2](#_Toc192861516)
* [3. 專案需求說明 3](#_Toc192861517)
* [4. 專案管理 6](#_Toc192861518)
* [5. 教育訓練 6](#_Toc192861519)
* [6. 驗收 7](#_Toc192861520)
* [7. 付款方式 7](#_Toc192861521)
* [8. 授權期間維護項目 7](#_Toc192861522)
* [9. 職業安全衛生管理 8](#_Toc192861523)
* [10. 資通安全要求 8](#_Toc192861524)
* [11. 個資保護要求 10](#_Toc192861525)
* [12. 建議書製作規則 11](#_Toc192861526)
* [13. 內容釋義附則 12](#_Toc192861527)
* [14. 聯絡資訊 12](#_Toc192861528)
* [15. 附件 12](#_Toc192861529)
1. **專案描述**
	1. 專案名稱

本專案名稱為臺灣基督教門諾會醫療財團法人（以下簡稱甲方）「網路微切分管理系統建置」（以下簡稱本專案）。

* 1. 專案目標

網路微分段技術能細化權限，並提升應用程式控管精準度；能補足傳統防火牆的不足，以動態的管理模式提升院內網路環境使用的的安全性。為強化機構主機間的網路安全架構，降低攻擊面，防止勒索軟體及進階持續性威脅，提供可視化安全策略管理並實現零信任網路存取策略，阻止未經授權的存取，確保企業資產的安全，降低橫向移動攻擊的風險。

* 1. 專案期程
		1. 專案期限：簽約後120日內完成交付及全案驗收。
		2. 本專案決標前如因故暫緩、延期或變更需求，甲方將另行通知，投標廠商不得提出要求相關損失責任。
	2. 名詞定義
		1. 時間：以下本專案所稱「日、時、分」，皆以 □日曆時間　☑工作時間 為計。。
		2. 驗收完成日：指完工後經甲及廠商雙方通過驗收簽名日。
		3. 年度業務正常運轉率：1-(系統非規劃性失效分鐘數 / (365\*24\*60) )
		4. 臺灣基督教門諾會醫療財團法人：包含美崙總院、壽豐分院及所屬相關機構。
		5. 美崙總院：定義為臺灣基督教門諾會醫療財團法人門諾醫院。
		6. 壽豐分院：定義為臺灣基督教門諾會醫療財團法人門諾醫院壽豐分院。
	3. 廠商資格
		1. 非經濟部投資審議委員會公告之「陸資投資資訊產業事業清冊」廠商。
		2. 營業項目具資訊軟體服務且資本總額新台幣3.5億元以上之公司行號。
		3. 須為採購標的之原製造廠商或原廠授權之經銷商
		4. 廠商須有國內建置導入經驗之實績。
		5. 技術維護人員需有原廠授權認證資格。
1. **現況說明**
	1. 設備環境
		1. 備有VMweare ESXi主機環境。
		2. 醫療相關儀器設備及無線監測傳輸儀器等。
		3. 資訊網路通訊相關設備
	2. 系統主機
		1. VMware vSphere作業系統主機。
		2. Windows Server作業系統主機。
		3. Oracle Solaris 作業系統主機。
		4. Linux Base作業系統主機。
		5. IBM AIX作業系統主機。
		6. Kubernetes作業系統主機
	3. 資料庫系統
		1. Oracle資料庫。
		2. MS-SQL資料庫。
	4. 主控台伺服端：甲方自備VMWare虛擬伺服器環境，可提供為網站或應用程式伺服器。
2. **專案需求說明**
	1. 導入範圍 (依提供之數量作為定案)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Core主機** | **版本** | **台數** | **Endpoint單位** | **作業系統版本** | **台數** |
| Solaris | 5.11 | 4 | IDS | Windows 11 | 20 |
| AIX | 7.2 | 4 | 醫 資 部 | Windows 11 | 4 |
| CentOS | 6.8 | 1 | 病 歷 室 | Windows 11 | 21 |
| 7.9 | 2 | 資 訊 室 | Windows 11 | 35 |
| 8.5 | 3 | 儀器(桌機)設備 | Windows | 43 |
| Ubuntu | 14.04 LTS | 1 | Endpoint Reserve 10% | 12 |
| 22.04 | 3 | 總 計 | 135 |
| Windows Server | 2008 R2 | 8 |
| 2012 | 17 |
| 2012 R2 | 21 |
| 2016 | 16 |
| 2019 | 28 |
| 2022 | 57 |
| RHEL | OpenShift | 4 |
| Core Reserve 10% | 16 |
| 總 計 | 185 |

* 1. 系統說明
		1. 目標功能
			1. 零信任架構支援：提供基於身份的存取控制，防止橫向移動。
			2. 動態策略定義及自訂：支援基於工作負載、使用者和應用程式的安全策略。
			3. 網路流量可視化：提供網路流量監測及即時可視化。
			4. 基於標籤的存取控制：自動調整策略，無需修改 IP 位址或 VLAN。
			5. 無須代理架構選項：支援網路方式與工作負載的部署模式。
		2. 可靠性功能
			1. 代理程式的啟動、停止或重新啟動，都不影響其安全防護功能且不影響系統穩定性。
			2. 代理程式安裝後，可不重新啟動系統。
			3. 可記錄所有安裝代理程式的設備之連線資訊（如 IP 和 Port）。
			4. 系統需內建的多節點架構備援機制。
			5. 代理程式與系統功能保持獨立性，移除代理程式後，不會影響原有防火牆設定，無需重新啟動設備即可繼續運作。
			6. 代理程式採用User Space方式設計，不影響系統運作，資源佔用低」。
		3. 安全性功能
			1. 根據歷史連線紀錄，自動生成微切分政策建議。
			2. 標籤化的管理方式，可對異常設備使用政策規則進行隔離。
			3. 對於高風險埠（如 SMB 或 RDP），系統提供自動偵測與阻擋的功能。
			4. 系統的部署不需改動現行網路架構。
			5. 提供風險管理面板，協助計算與降低高風險連線的影響。
			6. 需提供自動偵測核心服務(CoreServeice)功能，包含服務名稱、信心度及Port號。
			7. 提供防篡改能力，以避免人員手動調整本機規則。
			8. 提供動態流量加密功能，確保資料傳輸的安全性。
		4. 管理功能
			1. 代理程式在待命模式下記憶體消耗不超過 100MB，且不影響設備效能。
			2. 系統日誌傳輸資料量控制在每日10-15MB。
			3. 在同一管理平台下，可監控伺服器端、客戶端及雲端環境，並依不同視角(依環境、角色、應用系統、地點)可視化看到網路連線資訊。
			4. 無論設備是否離開企業網路，端點仍能持續受到保護。
			5. 支援管理規模從 2,500 台至 25,000 台以上的設備，確保穩定運行。
			6. 需支援Role-Based Access Control (RBAC)訪問管理，根據使用者的角色與範疇限制管理權限，完整記錄所有帳號操作與變更行為。
			7. 系統內建REST API，可供進行資料檢索或推送，以多樣化的客製管理需求。
			8. 支援將日誌資料輸出至 SIEM 平台進行分析，提供多種格式（如 JSON、CFE 或 LEEF）。
		5. 事件回應
			1. 當事件發生時，經甲方聯繫乙方後，乙方以電子郵件、電話、視訊會議或雙方事先議定之方式協助甲方處理事件。
			2. 若事件無法透過上述方式解決，甲方與乙方協調派員至指定地點處理事件。
	2. MNC（Multi-Node Cluster）規格 (2 x 2 small 架構)下方由甲方提供
		1. VEN (託管) / workloads (工作負載)數量上限，總數12,500
* 2,500 VENs / 10,000 workloads
	+ 1. 核心數與時脈速度：
		- 每個節點 4 核心 (vCPU)
		1. 記憶體：
		- 每個節點32GB
		1. 儲存裝置容量：
		- 核心節點：硬碟最小容量： 50GB
		- 資料節點：硬碟最小容量：硬碟一：250GB、硬碟二：250GB
	1. 系統軟體相容性
		1. VEN (Agent) Support
			1. Core OS
				1. UNIX作業系統

IBM AIX、Oracle Solaris。

* + - * 1. Windows作業系統

Windows Server

* + - * 1. Linux作業系統

Red Hat Enterprise Linux (RHEL)

CentOS、Ubuntu、Oracle Linux

SUSE Linux Enterprise Server (SLES)

* + - * 1. K8s作業系統

Kubernetes

RedHat OpenShift。

* + - 1. Endpoint OS
				1. Windows作業系統及版本

Windows 11

Windows 10 22H2 Build 19045

Windows 10 21H2 Build 19044

Windows 10 21H1 Build 19043

Windows 10 SAC 20H2 - Build 19042.630

Windows 10 2004 Build 19041

Windows 10 1909 Build 18363

Windows 10 1809 LTSC

Windows 10 1903 SAC Build 18362.239

Windows 10 1809 SAC Build 17763.437

Windows 10 1511 LTSB

Windows 8.1

Windows 7

* + - * 1. MAC 作業系統及版本

MacOS 15 (Sequoia)

MacOS 14 (Sonoma)

MacOS 13 (Ventura)

MacOS 12 (Monterey)

MacOS 11 (Big Sur)

* 1. 教育訓練本法人機構資訊部門能完整執行下列工作。
		+ 1. 系統執行前，須評估作業方式及期間對院內環境之影響。
			2. 確認不導致院內系統服務中斷。
	2. 系統架構
		1. 伺服器須配合甲方 VM 。
1. **專案管理**
	1. 廠商須於簽約2星期內召開專案啟始會議，向甲方說明專案執行計劃書，並至少每2星期召開一次定期專案會議；除此例行會議外，甲方有權要求廠商隨時提供相關工作資料及召開臨時會議，廠商不得拒絕或藉故拖延。
	2. 廠商須就甲方環境並評估相關資源風險後，規劃並實施各階段建置時程。若遇需變更 需求規格或合約之時程，則須先召開專案會議取得協議，再經甲方確認同意後實施。
	3. 系統建置應按複選議價表或最後議價文件及徵求建議書說明文件(詳附件)，惟建置過程中會因甲方工作流程及雙方資訊技術考量而異動原需求，故最終驗收功能與介接項目，須於驗收前經雙方討論，並由甲方使用單位確認，異動項目請廠商製表說明之。
	4. 雙方應依照建置計劃書所訂之施工責任介面施工。
	5. 本專案所須之資源與人力，包含成立專案小組及擬定本標的物之建置計劃書、佐證資料範本等相關文書、行政作業均由廠商負責，並依進度需要增加人力。
	6. 廠商必須選派本專案負責人及相關負責人參加，會中必須由本專案負責人提報目前工作進度及所遭遇問題之解決方案。
	7. 廠商必須於標的物建置完成上線測試日起，提供系統維護人\_2\_名駐甲方\_3\_日 ☑(5x8)　 □ (7x8)□(7x24)，期間廠商如有未到場情事發生，則將依其未在場時數順延，直到駐點期滿止。
	8. 本專案進行中，甲方有權要求提出更換不適任之專案人員，廠商不得藉故拖延及拒絕。
	9. 執行本專案期間，廠商同意甲方得視狀況要求廠商人員在甲方所提供之場所工作。
	10. 廠商須提供建置過程之文件，如會議紀錄及交付驗收時檢附之文件。各項文件共享方式須符合甲方保密及資安規範，文件內容除非有必要否則不應含有個資。
	11. 因甲方因素延誤相關交付期程，得於10日前通知更改完廠商成日期，且不計入廠商遲延。
	12. 廠商因不可抗力之事由（如天災、地變、罷工、戰爭）及其他非可歸責於廠商之事由，致使延誤本約完成期限，廠商應於專案會議通過後以正式公函提出申請，自該等事由消滅日起，順延同等期間交付各工作項目，不計入廠商之遲延。
2. **教育訓練**
	1. 廠商須於交貨後、驗收前，依建置計劃書所訂之教育訓練計劃，配合甲方時間、地點，為相關人員進行包含但不限於以下的操作及維修教育訓練，並得配合甲方實際需求延長教育訓練時數。
		1. 系統操作訓練：□無；☑至少\_1\_梯次，每次1小時以上。
		2. 故障排除訓練：□無；☑至少\_1\_梯次，每次1小時以上。
	2. 教育訓練課程辦理前，廠商應於上課前7天交付足夠數量之教材及講義書面或電子檔、簽到表，供上課學員使用及作為驗收依據。若參加原廠訓練，則廠商須負責為甲方安排所有相關事項。
	3. 廠商所有提供之教育訓練課程需配合導入甲方E-learning課程，並於保固維護期間，依甲方通知持續提供相關訓練課程。
3. **驗收**
	1. 系統軟硬體設備若於交貨時停止生產或升級，經甲方負責人同意後廠商得以功能最新且不低於本標的物所定之規格所需之產品替換。
	2. 交付標的物之規格、數量、時程應完全符合本案要求，除本條第一項之情形外，如有不符者，甲方有權要求廠商更換或補足之，廠商不得異議。更換或補足須於雙方議定時間內完成交付，廠商如末能於期限內完成手續時，視同逾期交貨。
	3. 廠商應免費提供甲方因執行驗收程序所必要之一切人員及設備，如廠商無法提供時，甲方得聘任第三者為之，其所需費用由廠商負擔，並由廠商貨款中扣除。
	4. 本案完成系統上線後，通過試運轉30日後始得辦理驗收，試運轉(驗證)期間異常改善，廠商應接獲甲方通知後，於 7 日內完成改善並於改善後次日起驗證 7 日無異常方視為完成改善。
4. **付款方式**
	1. 本專案交付期程依下列約定辦理：

|  |  |  |  |
| --- | --- | --- | --- |
| 期別 | 項目 | 檢附文件 | 請款額度 |
| 一 | 完成簽約 | ☑於啟始會議後一周內提供建置計畫書 | 總價金30%(新台幣X元整) |
| 二 | 簽約後90天內，完成系統建置 | ☑功能測試計畫及驗證報告☑版權證明及軟體授權證明 | 總價金30%(新台幣X元整) |
| 三 | 系統上線經試運轉30天無誤及完整教育訓練 | ☑系統驗收清單文件☑教育訓練明細佐證文件☑教育訓練教材及操作手冊電子檔 | 總價金40%(新台幣X元整) |

1. **授權期間維護項目**
	1. 供單一聯絡窗口事故排除及技術諮詢服務，該員須為廠商專任人員及通過原廠認證資格；人員年資2年以上者。
	2. **授權期間**：
		1. 除天然災害或不當操作造成損壞外，提供標的物□硬體 年；□電池 年；☑軟體 1 年之免費維護保固、功能訂閱、授權及升級等服務。
	3. 定期維護：
		1. 維護項目：

☑軟體維護須每季定期至維護標的所在地，進行現場或遠端維護服務，包含系統效能、資源耗用等分析及調校。

□硬體維護須每季定期至維護標的所在地，進行現場維護服務，其範圍包括清理、調整、檢視和測試等並免費更換正常使用下損壞之零件。

* + 1. 廠商應於每次維護完成後，提供甲方維護、建議事項，並由雙方簽名確認維護紀錄。
		2. 現場維護服務後於維護結果會議報告，包含：維護項目、系統運行狀況、系統資源使用狀況等。
		3. 廠商應於每年度期末提供次年度維護計劃。
		4. 停機維護須經甲方同意後執行，廠商應以不妨礙甲方正常工作時間為原則。
	1. 服務水準：
		1. 廠商保證維護標的年度業務正常運轉率達99%以上，除外情況：端末設備、甲方例行性、有預警計畫性停機或地震、火災等天然災害因素，則不計入系統中斷時數。
		2. 提供 □5x8　□7x8　☑7x24小時報修服務。接獲技術諮詢或維護請求時，得以電話、電郵或通訊軟體回應及使用遠端連線方式處理，連線方式由甲方提供，且須符合甲方之管理規範。如無法透過電話、電郵、通訊軟體或遠端連線方式處理時，依下述服務水準要求現場維護。
		3. 情況等級由甲方判定或並依現場情況之變化提升或降低故障等級：

|  |  |  |  |
| --- | --- | --- | --- |
| 狀況 | 情境 | 回應支援方式 | 完修期限 |
| 緊急 | 影響全院事件 | 30分鐘內 | 現場或遠端支援 | 接獲通知起4小時內完修 |
| 嚴重 | 設備或軟體故障，系統已無法維持高可用性狀態或營運持續計畫環境處於失效狀態 | 4小時內 | 現場或遠端支援 | 接獲通知起4日內完修 |
| 一般 | 弱點修補、系統設定調整、報表提供等 | 24小時內 | 現場或遠端支援 | 接獲通知起20日內完修 |

1. **職業安全衛生管理**

廠商在甲方作業期間，應遵守甲方管制相關規定及職業安全衛生相關法規並做好一切安全衛生措施，如廠商人員發生意外或職業災害等，屬可歸責於廠商，由廠商負責。

1. **資通安全要求**
	1. 有關雙方之專業技術、病人隱私、業務機密(含全部文件合約內容及發票金額等），雙方保證不得洩漏或交付第三者。
	2. 資安防護分級：
		1. 依據「資通安全責任等級分級辦法」揭示，本系統參照其分級原則，評估系統等級為「**S**」。【註：「**＊**」未涉及資通安全應用軟體開發】
		2. 系統防護基準如SSDLC採取措施及驗證查核表(**詳附件**)。合約期間廠商須維持維護標的評估系統等級為「**S**」且配合甲方不定期進行查核；惟如查核結果未達控制措施，廠商須於1個月內完成改善並達控制措施。
	3. 安全重點要求：
		1. 留在甲方施行單位內部處理機密性、敏感性或是關鍵性的應用系統項目。
		2. 執行事項應經甲方施行單位核准。
		3. 廠商發現疑似資通安全事件時，應即時通報甲方專案負責人，並提供資安事故相關資訊，於資安事故處理過程中，若涉及民、刑事法律行動，應進行蒐證與證據保留。
		4. 應與甲方共同管理和解決所有界定的問題及施行應用系統異動的管理程序。
		5. 應遵守資訊安全相關法律規範。
		6. 建置系統之鐘訊，須符合甲方時間來源同步要求。
		7. 建置系統之服務水準，須符合甲方營運持續計畫之業務回覆時間要求。
		8. 建置系統應提供各組件規格及版本，做為甲方建構管理之基礎資訊。
		9. 建置系統適用之作業系統版本，當有更新版本時，本系統之符合性須主動通知甲方。
		10. 應依甲方施行單位要求裝設防毒軟體。若該系統無法安裝時，應採取其他防護措施，且須經由甲方同意。
		11. 依據資通安全責任分級辦法附表十之源碼掃瞄要求，應配合甲方工具及監督下執行弱點與原始碼掃描。
		12. 若遇提供之服務變更時（例如：系統或設備更換、維護水準調整），應經甲方評估相關風險同意後再實施。
		13. 廠商應確保開發之系統或網站應用程式無留有任何形式之後門。
		14. 廠商欲連線甲方設備須事前經安全檢測，通過後方可使用。
		15. 相關硬體及軟體產生之任何資料，非經甲方同意，不得傳輸至甲方以外之網路(如：設備校正數據資料)。
		16. 依據資通安全責任分級辦法附表十之備份及營運持續要求，系統之資料備份與災難還原機制應配合甲方現有設備及環境進行規劃，制訂完善備份(援)程序及回復程序，詳細說明系統(含本系統使用之軟體、應用系統、系統內登錄之資料等)毀損之回復措施，系統如遭逢重大天然災害或人為意外時，能迅速重建系統及還原所有資料。廠商應配合甲方業務持續營運管理相關作業，並符合現況說明中之各項RTO及RPO標準。
		17. 甲方保有對廠商執行檢查及稽核的權利，甲方得依需要對廠商專案相關工作之執行、資料之處理及執行之紀錄，進行實地現場訪視或調閱資料，廠商應以合作態度及於合理時間內配合甲方或委託之專業機構稽核作業，提供相關書面資料或協助約談相關人員，廠商不得有異議。廠商經檢查或稽核結果發現不符合資安規範，須於接獲甲方通知期限內改善。
		18. 廠商於合約終止後，應歸還屬於甲方之資產(含硬體、軟體、資料和系統存取權限等)。
		19. 不得使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。
	4. 資訊系統原碼：
	基於保障甲方關鍵系統維運，得提供資訊系統原始碼，於每期期末無償交付甲方最新版次之資訊系統原始碼。惟套裝軟體可排此條款。
	5. 安全檢測作業：
		1. □ 原碼掃描安全檢測：
		依據資通安全責任分級辦法附表十之源碼掃瞄要求，新版程式發佈前須經過原碼檢測，每次程式更新上線前，廠商須先提交預備發佈之原始碼進行原碼檢測，並配合改善前兩級高風險問題，報告結果須無前兩級高風險等級問題，方可進行後續新版上線作業，整體作業流程須於1個月內完成。
		2. ☑ 弱點掃描安全檢測：
		依據資通安全責任分級辦法附表十之弱點掃瞄要求，甲方每年執行一次弱點掃描檢測作業，廠商須處理報告內容屬於前兩級高風險等級之弱點。直到甲方複掃報告中無前兩級高風險弱點才視為完成，整體作業流程於1個月內完成。
		3. □ 行動化應用軟體（Mobile App）安全檢測：
		本案若含行動化應用軟體（Mobile App），應通過經濟部工業局訂定之檢測項目，方可上架應用程式商店及提供民眾下載使用；前述檢測作業，應由符合經濟部工業局公告「行動應用App基本資安自主檢測推動制度」規範之認證合格檢測實驗室辦理，相關檢測費用由廠商負擔。（相關規範詳見行動應用資安聯盟網站 [ https://www.mas.org.tw ]）
		4. □ 滲透測試：
		依據資通安全責任分級辦法附表十之滲透測試要求，甲方每2年執行一次滲透測試作業，廠商須處理報告內容屬於前兩級高風險等級之弱點。直到甲方複掃報告中無前兩級高風險才視為完成，整體作業流程於1個月內完成。
2. **個資保護要求**

依據個資法及個資法施行細則，委託廠商配合辦理個資保護要求事項如下所述。

* 1. 廠商個人資料保護措施(二擇一)：

□ 廠商得提供其主管機關要求之「個人資料安全維護計畫」，說明委託蒐集、處理或利用個人資料之範圍、類別、特定目的及期間。廠商應依據個資法善盡個資保護管理之責。

□ 廠商應於簽約時向甲方進行個人資料保護管理狀況報告，並交付附件「委外廠商個資安全管理自評表」，甲方得視需要，進行實地稽核。

* 1. 廠商人員承辦或接觸甲方個資委外業務時，應簽訂「外部人員保密切結書(**詳附件**)」並遵守甲方「個資保護管理政策」相關規定。
	2. 廠商人員於受託業務執行期間若有異動，應事先通知甲方專案負責人，並重新簽署保密切結書。
	3. 廠商應防止個人資料洩漏並禁止盜用。
	4. 廠商禁止為合約範圍外之影印、複製、加工及利用。
	5. 廠商若要將個人資料相關作業再委託第三者，必須徵得甲方同意授權後，始得為之；複委託之機關亦應遵守本合約所要求之個資保護管理相關規範。
	6. 廠商應於合約終止或解除並啟動退場機制時，返還或銷毀/刪除因受委託而蒐集處理利 用之個人資料。
	7. 廠商若發現有違反個人資料保護法事件，必須即時通知甲方，說明事件的原委與應變措施，若有任何損失發生，則須負賠償責任。
	8. 合約期間傳遞之資料載體(包括但不限於隨身碟/可攜式硬碟/光碟片等儲存媒體)於使用完畢，必須確保資料已於載體中以無法復原方式刪除或銷毀。
	9. 應用系統內個資遭外洩或侵害情事，廠商必須於第一時間通報甲方，並說明目前已採取之因應措施與受影響程度。
	10. 甲方得視需要，邀請專家學者共同至廠商處所，就個資保護之實體安全、存取控制、通訊與作業管理及個人資料保護法施行細則第8條之要求，對廠商進行稽核作業，廠商不得拒絕。
1. 建議書製作規則
	1. 建議書撰寫大綱(詳附件)。
	2. 除 A3 尺寸繪製之必要圖表(說)外，建議用 A4 縱向紙張，內文應以中文由左至右橫式繕打撰寫(如有必要時，得以英文註記)。宜加目錄、編頁碼(下方置中)、加封面(不須編頁碼)並裝訂成冊。
	3. 封面應載明計畫名稱、投標廠商、申請機構(或團體)名稱，廠商、機構(或團體)之負責人姓名及計畫提出日期。
	4. 投標廠商應提出應提出建議書㇐式紙本 1 份(用印)，PDF(非影像檔)電子檔 1 份，併同其他投標文件投標及評選，所提建議書經提出後不得退換或更換補件。
	5. 若於建議書中引用相關書籍資料，應加註引用書籍名稱，且不得有「抄襲」情形。如未予登載加註，且內容有雷同之處，應視為抄襲，如未修正，不予採納。
	6. 製作建議書及合約簽訂前所費之成本，由投標廠商自行負擔，得標廠商之建議書所有權歸甲方。
	7. 甲方對投標廠商對投標廠商建議書中所提實績經驗或中所提實績經驗或專案小組成員之資歷有疑問時，得請投標廠商提出證明文件。
	8. 投標廠商對於本徵求建議書說明文件內容有疑義時，於本徵求建議書說明文件公告 7 日內以書面向甲方提出。
2. **內容釋義附則**

上述內容及相關附件有疑義時，以甲方解釋為主，甲方保有解釋及修改之權。

1. **聯絡資訊**
	1. 資訊室：黃硯侖/03-8241570/ianhuang@mch.org.tw
	2. 資源開發管理中心：黃月櫻/03-8241568/pur04@mch.org.tw
2. **附件**

☑　SSDLC 採取措施及驗證查核表

☑　外部人員保密切結書

□　個人資料安全維護計畫

☑　委外廠商個資安全管理自評表

☑　建議書撰寫大綱