

臺灣集中保管結算所股份有限公司

AWS Bedrock 雲端服務專案

規範書

數位暨資安部

中華民國 115 年 9 月

目 錄

壹、總則	2
貳、廠商資格	4
參、採購項目	6
肆、採購規格	7
伍、交付項目及時程	8
陸、驗收及付款方式	10
柒、保固與維護	12

壹、總則

- 一、本規範書係為臺灣集中保管結算所股份有限公司（以下簡稱本公司）「AWS Bedrock 雲端服務專案」（以下簡稱本案）而制訂。
- 二、為確保廠商有履行合約及提供完善服務之能力，廠商必須符合本規範書「貳、廠商資格」所訂之各項資格條件。
- 三、本規範書之「肆、採購規格」係對本案購置所須之軟、硬體設備規格，作整體概括性之說明及規範，其所訂定之各項設備性能及須具備之功能應視為最低要求，並提供廠商有義務提供超過最低要求之完整可供運轉設備，並可與現有環境整合運作。
- 四、廠商應依本規範書之「伍、交付項目及時程」完成交付，並至本公司指定之地點安裝並完成功能測試、組態設定與調校、等作業，且應與本公司現有環境整合運作。
- 五、廠商應依本規範書「陸、驗收及付款方式」進行驗收手續，另需配合本案設備之上線相關作業，倘有延遲之罰則，悉依合約規定辦理。
- 六、本規範書之「柒、保固與維護」規範廠商應提供之保固與維護服務項目，有與本公司簽訂買賣或維護合約者，以合約內容為準。
- 七、本案經履約完成、終止或解除時，廠商應返還、移交、刪除或銷毀履行本案而持有之資料，且不得有拷貝、複製或備份持有之行為，並要求受任人、受僱人、代理人及其他相關人員共同遵守。
- 八、廠商應遵守個人資料保護法、營業秘密法、資通安全管理法、本公司訂定之「資訊廠商應遵循之資通安全事項」(附件一)及本公司提供之相關作業規定；廠商參與人員均應受過適當之資通安全教育訓練。本公司認有必要時，得要求廠商派員參與本公司所舉辦之相關課程。
- 九、倘廠商與協力廠商知悉資通安全事件，除雲端委外作業另有約定外，應於 1 小時內通知本公司及採行之補救措施。
- 十、廠商須出具原廠授權之證明文件，並得註明本案執行之範圍及項目，委由協力廠商協助執行本案之作業。協力廠商或原廠協助執行作業造成本公司損害時，廠商應對本公司負賠償責任。

十一、廠商與協力廠商之資通訊設備，非經本公司同意不得與本公司資訊系統介接。

十二、本案廠商不得為主管機關核定生產、研發、製造或提供危害國家資通安全產品之廠商，廠商亦不得提供或使用危害國家資通安全之廠商產品；另參與人員均不得為大陸地區人民，並於受託業務範圍內，不得使用中國大陸廠牌資通訊產品(含硬體、軟體及服務) 作業。

十三、雲端服務資通安全規定：

(一)、廠商應為本公司取得雲端服務供應商同意查核之書面文件，並提供予本公司。本公司得自行委託，或與委託同一雲端服務供應商之其他機構聯合委託具資訊專業之獨立第三人，就雲端服務供應商執行本案受託作業情形進行查核。

(二)、本公司委託廠商或雲端服務供應商處理之投資人資料及其儲存地應依下列規定辦理：

(一) 本公司須保有其指定資料處理及儲存地之權利。

(二) 境外當地資料保護法規不得低於我國要求。

(三) 涉及重大性投資人業務資訊系統之投資人資料儲存地以位於我國境內為原則。如位於境外，除經主管機關核准者外，投資人重要資料應在我國留存備份。

(四) 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。

(五) 未經本公司同意之下，雲端服務供應商不得存取本公司儲存在雲端之資料，且不得為服務協議指定範圍以外之利用。

(三)、雲端委外契約終止，廠商應保證雲端服務供應商全數刪除或銷毀雲端留存資料，並出具資料完全刪除之證明，但合約終止後本公司仍賡續委託同一雲端服務供應商時，則不在此限。

(四)、廠商或雲端服務供應商對雲端委外作業若有重大異常或缺失應立即通知本公司，並應於知悉資通安全事件 30 分鐘內，通知本公司。

十四、對本規範書內容若有疑義，以本公司解釋為主。

貳、廠商資格

一、廠商須符合下列各項資格條件：

- (一)實收資本額須為新台幣壹仟伍佰萬元整（含）以上。
- (二)在臺灣之成立時間至少達3年以上。
- (三)領有權責機關發給之：
 - 1.經濟部公司登記證明書或公司變更（設立）登記表或法人登記證明文件或商業登記證明文件。
 - 2.最近一期有效之營業稅或綜合所得稅或機關所得稅納稅證明。
 - 3.票據交換機構或銀行於資格證明文件繳交截止日前一個月內所出具之非拒絕往來戶且最近一年無退票記錄證明。
- (四)廠商與協力廠商不得為經濟部投資審議司公告之陸資資訊服務業者（陸資投資資訊產業事業清冊公開於經濟部投資審議司網站<https://dir.moea.gov.tw/chinese/>）。
- (五)廠商與協力廠商不得為政府電子採購網公告之拒絕往來廠商(拒絕往來廠商名單公開於政府電子採購網站<https://web.pcc.gov.tw>)。
- (六)為本案各項設備之原製造廠商、代理商或經銷商。代理商或經銷商須檢具代理商或經銷商之證明文件，若經銷商之證明文件由代理商出具者，須另檢附其為合法代理商之證明文件。
- (七)廠商與協力廠商(原廠除外)應提出資通安全管理措施自我說明（附件二）或通過我國標準法主管機關委託機構認證之機構出具之有效驗證報告，證明具備完善之資通安全管理措施。
- (八)廠商應配置至少 1 員經適當之資格訓練或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。
- (九)廠商須提示其參與人員名單及其有效之資通安全證照或最近一年內參與資通安全訓練課程證明之一項，並由本公司檢核其勞工保險或在職證明文件，廠商如需更換本案參與人員時，應事先向本公司提出接替人員名單及其符合本規範書規定文件，供本公司審核同意後始得更換。
- (十)廠商最近二年內未發生資通安全事件者，應出具未發生資通安全事件

之切結。廠商最近二年內曾發生資通安全事件者，應出具書面說明，內容涵蓋資通安全事件通報、調查、處理、改善措施辦理情形，以及切結各項作業均依法規法令與公司程序規定辦理，相關風險並已排除等事項；改善措施尚未完成者，廠商應增列說明對本案履約之影響。

前述廠商出具之切結文件需通過本公司審核，方可參與本案。

二、廠商所提資料、文件，如經證實係偽造、變造或不實者，本公司除得依法處理外，並取消廠商之承攬資格。

參、採購項目

本案採購項目之品名及數量說明如下，其詳細型號或規格請參閱「肆、採購規格」。

- 一、AWS Bedrock 雲端服務。
- 二、AWS Bedrock 雲端服務之設定服務。
- 三、AWS Bedrock 雲端服務之諮詢服務。

肆、採購規格

本案合約期間自簽約日起至 116 年 12 月 31 日止，採購項目品名之型號或規格如下：

一、AWS Bedrock 雲端服務(詳 <https://aws.amazon.com/tw/bedrock/>)。

二、使用 AWS Bedrock 雲端服務設定服務項目如下：

項目	說明
設定組織架構與帳號	建立管理帳號、Bedrock 使用帳號、日誌存查帳號，包含「日誌存查帳號」，集中記錄所有系統操作日誌。
護欄	套用組織護欄(SCP)，設定本公司核准之對外 IP 才能使用 AWS 平台（包含登入主控台與呼叫 Bedrock）。
統一身分	建置統一帳號管理機制，禁止共用帳號。
費用管理	設定標籤機制，依部門(可多選)或使用者(可多選)產出 AI 費用報表，並設定費用上限提醒、停用及調整等功能。
AI 模型與聊天介面	於指定 AWS 區域開通所需之基礎模型（如 Claude），並以 Claude Code（VS Code 擴充功能）作為工程師端的對話與開發輔助介面，提供安裝設定、身分驗證串接（IAM/SSO）之導入協助；同時透過 Amazon Bedrock Agent Core Gateway 的 Web Search Tool（以 MCP 協定整合至 Claude Code）啟用網際網路搜尋功能。
對話日誌留存	系統完整記錄使用者與 AI 對話之提示詞與回覆內容，並提供日誌留存與匯出機制。
資料隱私與模型訓練限制	廠商需設定及保證，所有透過系統輸入之內部程式碼與機密資料，不會被 AWS 用於訓練其基礎模型。

項目	說明
管理員手冊	教育訓練及管理員使用手冊。

三、使用 AWS Bedrock 雲端服務之諮詢服務。

伍、交付項目及時程

一、廠商須於簽約後 75 日（含）內完成交付，交付項目如下：

（一）本規範書之「參、採購項目」。

（二）雲端服務業者同意查核之書面文件。

（三）提供 AWS 出具本案之 Bedrock 公有雲服務環境 99.9%以上可用度(SLA)保證證明文件。

二、交付之文件至少二份（紙本或光碟，若交付文件為光碟，內容需經過本公司掃毒並留存檢測結果證明）。

三、如本公司與廠商終止本案合約，廠商應保證雲端服務供應商全數刪除或銷毀雲端留存資料，並出具資料完全刪除之證明，惟委外同一雲端服務供應商則不在此限。

四、使用諮詢服務後，廠商需提供諮詢服務題目及開始處理時間，以利後續驗收。

陸、驗收及付款方式

一、驗收方式：

- (一) 設定服務：廠商應於簽約後 75 日（含）內完成本案「伍、交付項目及時程」所定一、二、及三、之服務及交付全部項目，經本公司確認驗收無誤。
- (二) 諮詢服務：於諮詢後，廠商應提供本案「伍、交付項目及時程」之四、所訂之文件，經本公司確認驗收無誤。

二、付款方式：

- (一) 設定服務費：於簽約後 75 日(含)內完成本案「伍、交付項目及時程」所定一、二、及三、之服務及交付全部項目，經本公司確認驗收無誤後支付。
- (二) 雲端服務費：廠商每月應檢具發票與前一月份之雲端服務使用量及依台灣亞馬遜網路服務有限公司雲端服務牌價(以下稱原廠牌價)計算之費用清單向本公司申請付款，本公司依該月雲端服務使用量及原廠牌價之比例計算並核對無誤後，支付該月雲端服務費(加計 5%營業稅)。
- (三) 諮詢服務費：於本案首期及最後一期支付雲端服務費時，各支付 50%；本公司確認無誤後以即期票據或電匯(匯費由廠商負擔)方式支付。

柒、保固與維護

- 一、 本公司於合約期間內應享有問題諮詢服務、諮詢時段為【星期一至星期五，以及本公司之彈性上班日（以政府或臺灣證券交易所公告者為準）八時三十分至十七時三十分】。廠商於維護時段內接獲本公司通知後，須提供本案標的相關問題諮詢服務及處理。
- 二、 廠商未能履行前述任一條款規定之情事者，本公司有權按合約規定計罰違約金及請求損害賠償。
- 三、 乙方對雲端委外作業若有重大異常或缺失應立即通知本公司，並應於知悉資通安全事件 30 分鐘內通知本公司。

資訊廠商應遵循之資通安全事項

- 一、廠商發生資通安全事件(以下稱資安事件)涉及本公司委託業務範圍時，應於知悉資安事件後 1 小時內(屬雲端委外服務業務者，應於知悉資安事件後 30 分鐘內)通知本公司事件發生過程與評估影響範圍，本公司於接獲通知時應判定資安事件等級與告知廠商，廠商並應採取適當之應變措施與辦理下列事項：
 - (一) 一、二級資安事件應於知悉後七十二小時內，完成損害控制或復原作業，並通知本公司。
 - (二) 三、四級資安事件應於知悉後三十六小時內，完成損害控制或復原作業，並通知本公司。
 - (三) 完成損害控制或復原作業後，應於 1 個月內完成調查、處理及改善報告提供本公司。
- 二、廠商於公開資訊觀測站發布發生資安事件，應於發布當日通知本公司。
- 三、本公司委託業務之相關資訊(包含但不限於規範書、程式碼、元件與專案文件)應妥善保管，並僅提供專案團隊人員於執行本公司委託業務時使用，惟經本公司同意者不在此限；本公司委託業務之相關文件或其內容，如遭洩漏或不當使用，應比照資安事件啟動通報與應變機制。
- 四、處理本公司委託業務範圍時，廠商應遵守下列事項：
 - (一) 資通安全管理法、資通安全管理法施行細則、個人資料保護法、個人資料保護法施行細則及 ISO/CNS 27001 之規範。
 - (二) 實施資通安全認知宣導與教育訓練，應涵蓋社交工程與本「資訊廠商應遵循之資通安全事項」要求內容，以強化人員資通安全意識、降低誤觸社交工程之機率，與瞭解自身資通安全權責。
 - (三) 制訂適當之安全管控措施，避免未經授權之存取、防範系統遭受破壞，以及確保業務資料之機密性、完整性及可用性。
 - (四) 資訊系統之規劃，應考量安全需求，並於設計、測試、變更與維護各階

段，採取適當之安全管控措施。

- (五) 建立監控、通報與應變機制，以及時發現資安事件並有效的因應處理。
- (六) 涉及本公司委託業務之程式碼、元件與資料**夾名稱**等，不得使用可直接識別本公司之文字(如集保、TDCC 等)、**圖像/符號(如集保 LOGO)、影音等**，惟經本公司同意者(如應用系統功能擴充沿用舊有元件、**專案文件等**)，不在此限。
- (七) 使用公用雲執行本公司之委託業務時，應檢附公用雲相關安全設定(如權限最小化)說明文件，並取得本公司書面同意，方可使用。
- (八) 與委託業務相關之開發環境，定期辦理安全性檢測，檢測發現之高風險以上之弱點項目，應研議因應措施與持續追蹤改善。
- (九) **禁止使用中國大陸廠牌資通訊產品[含軟體、硬體及服務(含生成式 AI 程式如：Deepseek 等)]。**

五、若有公司組織調整、業務重大異動等(如:團隊變更)，於得知異動執行前主動通知本公司。

六、資訊相關設備及帳號之使用與管理規定

(一)資訊系統委外廠商或委外購買人力之派駐人員

1. 應使用本公司所提供之電腦設備與各項資源，且不得移作與專案無關之用途。
2. 本公司得派員進行電腦病毒、系統弱點、後門程式偵測等相關安全檢查工作，以維護系統作業安全，如發現有或評估可能發生影響資通安全之情事時，本公司得隨時要求廠商停止作業或撤出本公司。

(二)所有委外廠商人員

1. 不得使用中國大陸元件，且使用開源軟體或第三方元件應先取得本公司同意。
2. 廠商未遵守相關規定而導致本公司設備遺失、毀損或有損及本公司權益之情事，廠商應負賠償之責。
3. 倘持有本公司帳號，帳號持有人應盡妥善保管帳號密碼之責，帳號僅

限於該帳號持有人本人使用，亦不得使用非本人帳號。如帳號密碼有外洩疑慮或懷疑遭受未經授權存取，除儘速更換密碼外，並應立即通知本公司。

4. 廠商人員因業務需要進入本公司資訊系統執行各項維護作業時，應由本公司持有該系統帳號權限之主辦組陪同人員登入系統，並由廠商人員從旁協助進行維護作業。
5. 廠商人員使用之資訊設備(含伺服器、個人電腦、筆記型/平板電腦等)，倘涉及本公司委託業務時，應辦理下列事項：
 - (1) 建置防毒機制與適時更新病毒碼，並適時進行病毒掃描。
 - (2) 適時執行作業系統及軟體版本更新作業，與版本修補作業。
 - (3) 電腦設備應有帳密及螢幕保護機制，以避免資料外洩。
 - (4) 可攜式電腦設備(筆記型/平板電腦、USB...等)應有適當之保護機制，避免遭非設備持有人員開啟。

七、電腦機房或管制區域進出管理

- (一) 資訊系統委外廠商或委外購買人力之派駐人員，負責資訊系統開發與維護之派駐人員，應於本公司指定之廠商測試區進行作業；負責辦公室自動化設備安裝與維護之派駐人員，應於本公司同仁陪同下，於指定之工作時間及場所進行作業。
- (二) 需先經由權責部門組級以上主管核准，填寫「電腦機房進出登記簿」或「管制區域人員進出/使用登記簿」後，始得由相關授權人員陪同進入本公司管制區域；惟因應緊急事故處理時，得先填寫前揭登記簿後進入，事後再由權責部門組級以上主管於登記簿補行簽章。
- (三) 本公司電腦機房或管制區域作業區內禁止將行動電話及具攝錄功能之設備攜出(入)，因業務所需之電腦相關設備，於攜出(入)電腦機房或管制區域前，須獲得權責部門組級主管核准，並於「電腦機房資訊設備進出申請單」或「管制區域人員進出/使用登記簿」中的備註欄位詳細註明後，始可准許攜出(入)。

八、其他

- (一)進入本公司前，應至警衛執勤處辦理換證事宜，用以刷卡進出指定作業場所，臨時證遺失或毀損應向本公司主辦部門申請補發，並繳交補發費用。
- (二)資訊系統委外廠商或委外購買人力之派駐人員進駐廠商測試區，應先完成「保密同意書」（公司版）、「保密同意書」（員工版）、「測試區廠商派駐人員專用」之告知聲明。
- (三)本公司管制區域內不得攜入或存放具磁性、放射性、易燃性、易爆性等非工作需要物品，且禁止與處理電腦業務無關之一切行為，本公司購置之各類電腦設備，非經核准，不得攜出本公司。
- (四)軟、硬體交付項目需經主辦單位檢測不含惡意程式(如後門或木馬程式等)，或由廠商提供不含惡意程式之掃描報告或承諾書。
- (五)應確實了解並遵守本公司資通安全政策(請參考本公司官網)及本公司提供之相關作業規定。
- (六)應配合本公司通知，並依本公司規定方式辦理資通安全自評作業。

資通安全管理措施自我說明

附件二

廠商應提供下列各項說明 (如有佐證資料需檢附):

- 一、 資安事件之預防、通報及應變辦法。(例如：訂定緊急應變、通報程序或其他相關管理機制)
- 二、 資通安全稽核機制。(例如：內部稽核計劃或其他相關稽核機制)
- 三、 資通安全教育訓練。(例如：最近一年一般使用者及主管內、外部課程訓練紀錄等)
- 四、 資通安全技術面防護。(例如：帳號管控、防毒軟體、網路防火牆、電子郵件過濾機制或其他相關防護機制)

此致

臺灣集中保管結算所股份有限公司

公 司：

負 責 人：

統一編號：

地 址：

電 話：

中華民國

年

月

日