全國農業金庫數位金融身分威脅與生物辨識防禦情資服務規格及特別條款

全國農業金庫股份有限公司（以下稱本公司）數位金融身分威脅與生物辨識防禦情資服務（以下稱本案服務），其規格及特別條款規定如下：

甲、 規格

一、 一般規定

（一）投標廠商為公司法設立之公司、登記有案之法人、依法設立之營利機構。

（二）投標廠商應具備提供情資服務經驗，於投標時提出截標日前 2 年內之金融同業提供情資服務經驗之採購契約、驗收文件、維護合約或使用單位上線運作證明等任一文件影本。

（三）投標廠商通過 ISO 27001 或 CNS 27001 驗證，於議價時提出相關證明文件影本。

（四）投標廠商應具備金融同業風險威脅評估、資安健診、弱點掃描或滲透測試等任一項服務經驗。

（五）投標廠商應按投標金額 5%之現金、金融機構簽發之本票或支票、銀行保付支票、郵政匯票繳存押標金，得標後押標金轉為履約保證金，未得標者無息退還。履約保證金經履約完成無待解決事項後轉為保固保證金，保固期滿且無待解決事項後無息發還保固保證金。

（六）投標廠商如有政府採購法第 101 條所列之情事，經刊登於政府採購公報者，依同法第 103 條規定之期限內，不得參加投標或作為決標對象或分包廠商。

（七）本規格稱”以上”、”以下”、”以內”、”至少”、”高於”、”低於”俱含本數。

二、服務內容規格

（一）提供情資服務

主動針對本公司網路銀行系統運用間接驗證生物特徵技術、憑證外洩、身分冒用與身分鑑別弱點等項，蒐集資安威脅情資，進行分析與彙整，以作為評估與防範生物辨識風險之依據，並協助建立補償措施建議。

（二）定期提供分析報告

每月提供一份資料彙整服務月報，若當月無發現情資，則

提供其他金融產業情資分享。

(三)顧問諮詢服務

專案期間提供電話、電子郵件、遠端操作及人員到場等顧問諮詢服務。

乙、 特別條款

一、 得標廠商同意履行以下情事：

(一) 得標廠商履行契約不得違反法令強制或禁止規定、公共秩序及善良風俗，對本公司經營、管理及客戶權益，不得有不利之影響，並應遵守農業金融法、銀行法、洗錢防制法、個人資料保護法、消費者保護法、中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及其他法令之規定。得標廠商應本於善良管理人之注意義務辦理本契約事宜，契約如有履行不能或履行困難之虞者，應即通知本公司。

(二) 得標廠商應依本公司各項作業委外相關業務規章訂定之標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，建立消費者爭端解決機制，包含解決時程、程序及補救措施外，另應提供聯絡窗口及電話詢答服務。

(三) 得標廠商同意金融監督管理委員會、中央銀行、中央存款保險股份有限公司、農業部農業金融署等機關或依農業金融法第7條規定之機關及本公司自行辦理或委託獨立第三方單位進行辦理本契約相關事項之稽核或依金融機構作業委託他人處理內部作業制度及程序辦法進行本契約相關事項年度查核與稽核作業。得標廠商應提供本契約之應辦事項相關資料或報告,配合金融檢查或稽核,並於期限內提供相關資料或報告。

(四) 得標廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知得標廠商後終止或解除契約，本公司於主管機關命為終止或解除契約時亦同。

(五) 得標廠商履行契約應辦事項，對外不得以本公司名義為之，亦不得進行不實廣告，若違反致本公司受損，應負賠償責任。

(六) 本契約應辦事項若有重大異常、缺失或發現疑似資訊安全或個人資料外洩等異常事件或事故時，得標廠商應立即以口頭、電話等方式通知本公司，並配合本公司相關程序辦理異常排除及通報事宜,如必要應提供駐點服務。並於處理完成後，提供相關報告。

（七） 保密義務：

1. 得標廠商因履行本契約所知悉或接觸之一切有關本公司及本公司客戶之專案資料（包括但不限於需求訪談錄影、音檔、會議紀錄、系統文件、架構圖、原始碼及用戶個資等），均屬本公司之機密資訊應負保密義務，僅得揭露予為履行本契約目的而有接觸必要之得標廠商及其人員或分包商。本保密義務於契約終止、解除或期限屆滿後仍繼續有效。非經本公司事前書面核准，得標廠商不得將前述機密資訊上傳、儲存、輸入、處理或傳達至未經本公司核准之雲端平台、第三方協作工具、生成式人工智慧 AI 服務或外部公用網路空間。得標廠商應採取必要之安全措施，確保資料不被非法存取或外洩。如致本公司遭受損害應由得標廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。
2. 得標廠商於契約履行期間應提供得標廠商服務人員名冊（含公司簽章）及「廠商服務人員保密同意書」至本公司備查，且應加強對其聘僱人員之管理，包括人員進用、考核及處分等情事，以避免有不適任或有不法情事發生。

（八） 得標廠商提供本公司使用之軟硬體應為合法，如有第三者主張得標廠商提供本公司使用之軟硬體有侵犯智慧財產權時，本公司同意儘速以書面通知得標廠商，得標廠商應負責為本公司提出抗辯或和解談判，所有經法院判決確定或成立和解應由本公司負擔之費用、損害賠償及本公司因此所支付之費用（含委聘律師酬金）、所受之損害等均由得標廠商負擔。

（九） 因本契約應辦事項之性質、產品內容或服務（如訂閱制服務、客制化套裝軟體、商業應用軟體、電腦週邊設備採購等），得標廠商無法提供服務水準或補償性控制措施時，雙方之權利義務得依雙方協議內容另定之。

（十） 得標廠商不得將本契約或基於本契約所生之權利義務，全部或一部分轉讓或複委託予其他第三人，但經本公司事先書面同意者不在此限。

（十一）經本公司事先書面同意之複委託，其範圍及限制、條件均不得超出本契約；得標廠商應確認分包商具備資訊安全措施、遵循本公司資訊安全管理制度並簽署保密協議，如因分包商之不當行為致本公司發生損害時，得標廠商

應與分包商負連帶損害賠償責任。

(十二)得標廠商資訊安全責任：

1. 得標廠商須遵守本公司現有各項系統管理作業規定及安全管理規範,此外本公司保有對得標廠商執行稽核權利,包含稽核結果之改善追蹤機制,本公司可自行辦理或委託獨立第三方執行資訊安全訪視作業，或由得標廠商提供公正第三方之驗證報告。
2. 得標廠商於契約經終止、解除、完成履約後或其人員異動時(完成階段性任務或離職等情形)，得標廠商應完成本公司資訊資產與資料返還、移交、刪除或銷毀,並移除得標廠商於服務期間所取得之實體與邏輯存取權限，並保留執行紀錄。
3. 得標廠商如需使用自攜資訊設備,應經本公司檢核同意後始得使用，且不得連接本公司內部網路。
4. 得標廠商所提供之服務如發生變更,應於變更前主動以書面文件告知本公司相關事宜，包括但不限於契約變更、得標廠商組織重大調整(如：得標廠商與其產品或服務提供地、實質受益人或控制權來源國不符合國內相關規範要求)、業務重大異動或契約提前終止等;如得標廠商服務內容異動對資訊安全有所衝擊,得標廠商應重新協助本公司需求單位進行存取風險之辨識評估及對高風險變更之處置對策，並填寫相關風險評估表。
5. 因得標廠商及其人員或分包商之因素,導致發生資安事件或未達本公司資訊安全要求之服務水準時，應依契約所定罰則計付懲罰性違約金予本公司，若因此造成本公司相關損害,得標廠商應與其人員或分包商依契約內容負連帶賠償責任。

(十三)得標廠商禁止使用中國廠牌資通訊產品、軟體（如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等）、硬體（包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備）及資通訊服務。

(十四)得標廠商依本契約提供本公司服務時，如使用開源軟體，禁止使用高拘束性授權(如：AGPL授權)、中國開發套件或嚴重風險與高風險弱點套件。

(十五)得標廠商因履行契約應辦事項所應負之損害賠償責任，悉依民法及相關法令辦理。

(十六)得標廠商應遵循相關法令法規及其他適當資訊安全國際

標準。

(十七)得標廠商應提供第三方認證證明或公正第三方之驗證報告，如資訊安全管理國際標準要求或資訊安全管理系統國家標準（ISO/CNS 27001）有效證書；得標廠商若無法提供時，應提供資通安全管理措施或配合本公司自行辦理或委託獨立第三方執行資訊安全訪視作業。

(十八)得標廠商需指派專人配合本公司資訊安全要求，並負責督導本案得標廠商專案成員辦理各項本公司資訊安全要求事項，例如弱點掃描、滲透測試、源碼檢測、第三方元件檢測等，資安檢測發現之風險弱點項目，應配合本公司要求於期限內進行修正完成，本公司不另行付費。

(十九)應本公司業務需要，得標廠商對於所開發之應用軟體同意本公司使用並重製於本公司所購置之機器中，本公司不另行付費。

(二十)得標廠商應配合本公司於系統軟硬體換版時，協助辨識複雜度及影響範圍，提供風險影響評估報告與上線及復原計畫操作手冊。

(二十一)得標廠商應確實對其人員執行資訊安全教育訓練，並配合提供予本公司資訊安全教育訓練證明。

(二十二)本公司如因業務需要對得標廠商所提供之程式或文件得作適當之修改。

(二十三)得標廠商依本契約所提供之產品或服務提供地(包含對該產品或服務具有最終所有權之自然人或持有對提供該產品或服務之得標廠商超過25%股份或資本之控制權國家)，應非屬我國主管機關所列具風險或限制之國家(含自然人國籍)，倘經查證未符合主管機關法令規定及本公司有關資訊安全之規範或提供虛偽資訊，本公司得依契約約定解除或終止契約，並得依法追究其損害賠償責任。

(二十四)因可歸責於得標廠商而終止契約，本公司得要求得標廠商應將終止前已進行但尚未完成之工作成果及相關文件，依現狀交付予本公司，並同意本公司得就其未完成之工作成果自行或委由第三人繼續完成，得標廠商不得對該未完成之工作成果及相關文件主張任何權利。

(二十五)契約標的物於作業移轉至其他廠商或移回本公司時，得標廠商應提供系統遷移、資料處理之協助，如於移轉過程導致系統中斷，得標廠商應負中斷之賠償責任。

(二十六)得標廠商交付之資訊服務軟體(含客製化開發、套裝軟體、維護升級或整合組件），應依實際使用情形，辦理密碼技

術資產盤點；得標廠商於開發與交付階段，應針對軟體系統內所使用之密碼學演算法、金鑰管理機制、憑證及相關加密元件進行盤點，符合量子加密演算法最低強度，防止量子電腦破密，並提供「密碼技術資產清單（CBOM）盤點調查表暨切結聲明書」（以下稱CBOM調查表暨切結書），作為本案軟體應用規格及驗收之依據。

二、 報價

得標廠商以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項目	名稱	型號	數量	單價	金額
一	數位金融身分威脅與生物辨識防禦情資服務		1批	○○	○○○
二	顧問服務		1批	○○	○○○
合計					○○○

*以上報價應依規格內容報價（含稅）。

三、 交貨、安裝及測試

（一）得標廠商須自簽約次日起提供1年數位金融身分威脅與生物辨識防禦情資服務。

（二）如逾前項所訂期限，得標廠商須依照下列公式計付懲罰性違約金予本公司：

懲罰性違約金 = 契約總價款 * 0.1% * 逾期日數

如逾期超過前項約定期限1個月仍未提供本案服務時，除應依前述規定計付懲罰性違約金外，本公司得通知終止或解除契約之部分或全部，並沒入履約保證金。

（三）前開懲罰性違約金之累計總額以契約總價之20%為上限，本公司並得自契約總價或履約保證金中扣抵。

（四）本案服務配合各項檢測所需之檢測硬體及軟體，應由得標廠商提供並負責安裝與檢視，本公司不另行付費或提供相關設備。

四、 驗收與付款

（一）得標廠商於簽約次日，定期交付相關文件後，以每半年為一期，出具每月本公司簽認之服務證明文件，每期請領總價款之50%，經驗收後按期付款，共2期。

（二）應交付相關文件如下：

項目	文件名稱	形式	份數
1	針對網路銀行系統運用間接驗證生物特徵技術、憑證外洩、身分冒用與身分鑑別弱點等項，蒐集資安威脅情資，進行分析與彙整，以作為評估與防範生物辨識風險之依據，並協助建立補償措施建議。每月提供一份資料彙整服務月報，若當月無發現情資，則提供其他金融產業情資分享。	書面及電子檔	1

五、 維護及保固

得標廠商於專案期間，提供1年之諮詢與建議。

六、 得標廠商應對本案契約內容充分瞭解，並應依本公司之解釋切實執行辦理。

資訊安全與服務水準協定(SLA)罰則

一、資訊安全與服務水準規範：

項目	項次	項目	規範標準
資訊安全	1	資訊安全管理	如有洩密、疏失、管理不善等情事，致本公司遭致損失。
	2	存取控制及保全	因故意或過失導致本公司資訊資產遭不當取得、刪除或變更等情事。
	3	事件通報	引起本公司發生資訊安全事件且未即通報造成損失。
	4	威脅及弱點修補	系統重大弱點公布後或內部弱點掃描檢測未於規定之時間內修補完畢。
服務水準	1	系統可用性	每月以 95%以上的服務可用時間為服務承諾。
	2	客服支援時段	配合本公司營業日上午 9 點至下午 5 點。
	3	問題回應時間	得標廠商須於收到本公司通報後 1 小時內回應，並透過電話服務協助系統問題之判斷、偵錯與故障排除，如有進一步到場鑑定維護之必要，須於收到通報後 4 小時內（含交通時間）到場服務。
	4	復原點目標	發生故障時，將設備故障之服務狀態還原至其他主機繼續提供服務。

二、相關說明：

(一)得標廠商違反資訊安全與服務水準時，如須延長日期或非廠商之問題（不納入計罰），須經本公司同意。

(二)得標廠商違反資訊安全與服務水準時，每違反 1 次，本公司得按契約總價之 0.1%計算懲罰性違約金。

(三)得標廠商指派之專案負責人及工作成員，未經本公司同意，不得更換，如有未經本公司同意自行更換時，每更換 1 次得依契約總價之 0.1%計算懲罰性違約金。

(四)得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付之文件經本公司審閱，所發現錯漏處達 10 處以上，或業經本公司要求修訂仍未修訂者，本公司得按每字新臺幣 1,000 元計算懲罰性違約金。

(五)第(二)款至第(四)款之懲罰性違約金累計總額以契約總價之 20%為上限。如違約金違約金總額達契約總價之 20%時，本公司得通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。

(六)得標廠商依各款應付之懲罰性違約金可自契約總價、履約保證金或保固保證金中扣抵。