全國農業金庫網路銀行APP檢測服務（含iOS及Android）
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）網路銀行APP檢測服務(含iOS及Android)（以下稱本案設備）1批，其規格及特別條款規定如下：

甲、 規格

一、 一般規定

（一）本案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）本案廠商應具備本案議價日前1年內之國內銀行APP檢測服務經驗，並於議價時提出相關證明文件影本。

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

（四）本案廠商須為行動應用資安聯盟實驗室認證通過名單，並於議價時提出相關證明文件影本。

（五）本案廠商應具備資安健診服務、弱點掃描服務、滲透測試服務經驗。

（六）本案廠商應按投標金額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。

（七）本案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。

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

乙、 特別條款

一、 得標廠商同意履行以下情事：

（一）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。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）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）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。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）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）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，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. 廠商因履行契約應辦事項所知悉或存放於廠商雲端空間之一切有關本公司及本公司客戶等相關資料及內容，僅得揭露於本契約目的範圍內有接觸需要之廠商員工，廠商及其聘僱人員應保守秘密不得洩漏，並採取必要之安全措施，否則如致本公司遭受損害應由廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。
2. 廠商於契約履行期間應提供開發、維護（修）之服務人員名冊（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，包括人員晉用、考核及處分等情事，以避免有不適任或有不法情事發生。

（八）廠商提供本公司使用之軟硬體應為合法，如有第三者主張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廠商，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），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）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；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，廠商應與分包商負連帶損害賠償責任。

（十二）廠商資訊安全責任：

1. 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，或由廠商提供公正第三方之驗證報告。
2. 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），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. 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. 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、廠商組織重大調整、業務重大異動或契約提前終止等；如廠商服務內容異動對資訊安全有所衝擊，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，廠商應與及其人員或分包商依契約內容負連帶賠償責任。

（十三） 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） 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） 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） 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） 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；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） 廠商所提供之程式、檔案與軟體，無條件供本公司存查，惟不得公開予無關之第三者。於契約履行期間所開發應用程式與所交付軟體，廠商應善盡義務執行資訊安全檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、後門程式、間諜軟體及勒索軟體等）及隱密通道(Tunnel channel）等，並出具相關資安檢測證明文件。於上線前應清除正式環境之測試資料與帳號及管理資料與帳號，並採取防止電腦病毒散布之處置措施，以確保本公司之資訊系統安全無虞；如廠商未盡上述義務，致本公司因此所受一切損害（含本公司依法對第三人應負賠償責任及應給付之罰鍰），廠商應負賠償責任。

（十九） 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。

（二十） 應本公司業務需要，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。

（二十一）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。

（二十二）廠商依本契約提供本公司服務時，如使用開源軟體，應依該開源軟體之授權範圍，授權本公司利用，並以執行檔及原始碼共同提供之方式交付予本公司使用，廠商應於上線前交付開源軟體清單（包括但不限於開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文），及通過開源軟體檢測，本公司不另行付費。

（二十三）廠商所提供之程式若有採用第三方套件（非廠商自行開發之程式），應明列於系統維護手冊中，且交付驗收前應確認無已知公開的風險；於契約履行期間內若採用之第三方套件經揭露弱點風險，須配合本公司要求於期限內完成修正，本公司不另行付費。

（二十四）契約履行期間內，為解決第三方套件經揭露弱點風險之修正，其解決方法、範圍、期限，廠商應協助評估及處理，如係非廠商單方修正程式得以解決(如需作業系統、資料庫、產品升級或原廠產品已終結等)，且經本公司確認者，則不受前款規定限制，雙方得另議處理方法。

（二十五）廠商不得於提供之設備上做任何不當作業之行為及植入非法或足以損害正常作業與保密之功能，否則如致本公司遭受損害，應由廠商負賠償責任。

（二十六）廠商於上線前應配合本公司要求進行相關檢測，並提交相關無弱點檢測文件。如應用軟體程式應於上線前通過源碼檢測、系統及設備應於上線前通過弱點掃描、對外網頁版應用系統應於上線前通過滲透測試，本公司不另行付費。

（二十七）弱點檢測如因市場工具未能支援無法提出相關檢測文件，廠商應出具資訊安全聲明書。

（二十八）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。

（二十九）本公司如因業務需要對廠商所提供之程式或文件得作適當之修改。

（三十） 廠商若有破產、重整、解散、暫停營業或履行契約應辦事項有困難之虞者，廠商應依本公司指示交付本契約範圍內之程式原始碼外，另同意並授權本公司得逕行修改該程式原始碼。

（三十一）配合本公司進行營運持續計畫(BCP)演練。

（三十二）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。

(三十三)因可歸責於廠商而終止契約，本公司得要求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，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。

(三十四)契約標的物於作業移轉至其他廠商或移回本公司時，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，廠商應負中斷之賠償責任。

(三十五)履約期間遇資安事件時，廠商應辦理事項：

1. 知悉發生資安事件之通報並採取適當應變措施
   廠商知悉發生資安事件應於2小時內通知本公司（或接獲本公司通知2小時內），並採取適當之應變措施。逾時未完成，本公司得請求廠商按逾時時數，每小時支付契約總價款0.1%之懲罰性違約金，逾時未達1小時者以1小時計。
2. 完成損害控制或復原作業
   廠商應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業。逾時未完成，本公司得請求廠商按逾時時數，每小時支付契約總價款0.1%之懲罰性違約金，逾時未達1小時者以1小時計。
3. 調查及處理資安事件
   廠商完成損害控制或復原作業後，應於1個月內送交調查、處理及改善報告(或因應本公司所訂期限及指示事項提供協助調查處理相關事宜）。逾期未完成，本公司得請求廠商按逾期日數，每日支付契約總價款 0.1 %之懲罰性違約金，1日以24小時計，逾時未達24小時者以1日計。
4. 前開懲罰性違約金之累計總額以契約總價款之20%為上限。本公司並得自契約總價款、履約保證金或保固保證金中扣抵。如懲罰性違約金總額達契約總價款之20%時，本公司得通知廠商終止或解除契約之部分或全部，且不補償廠商所生之損失。

二、 報價

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	網路銀APP檢測服務(含iOS及Android) A.OWASP Top 10 Mobile APP Security Checklist L2檢測評估 B.經濟部工業局「行動應用APP基本資安檢測基準V3.2」 L3檢測		1批	○○	○○○
二	取得數位發展部數位產業署行動應用APP基本資安標章及合格證書(MAS標章)				
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）廠商須於簽約次日起8個月內完成網路銀行(個人網銀及企業網銀)滲透測試及APP檢測並取得數位發展部數位產業署行動應用APP基本資安標章及合格證書。

（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個月仍未完成時，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款之20%為上限，本公司並得自契約總價款或履約保證金中扣抵。

（四）本案設備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）廠商於簽約次日8個月內完成本案，交付相關文件後，由本公司派員辦理驗收，驗收合格後，支付契約總價款。

（二）應交付相關文件如下：

項目	文件名稱	形式	份數
1	1.取得數位發展部數位產業署行動應用APP基本資安標章及合格證書 2.出具OWASP Top 10 初測及複測評估報告 3.出具APP L3 初測及複測評估報告 4.工作說明書	書面及電子檔	1

五、 維護及保固

廠商於本公司完成各年度驗收之次日起，無償提供1年之諮詢與建議。

六、 廠商應提供本案相關教育訓練4小時並詳列於工作說明書，本公司不另行付費。

七、 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。

附件

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規範時，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)款之懲罰性違約金總額以契約總價之 20%為上限。如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。