

全國農業金庫
企業網銀及個人網銀 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）企業網銀及個人網銀 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” 具含本數。

乙、 特別條款

一、 本案設備維護工作應由得標廠商承擔。

二、 得標廠商同意履行以下情事：

- （一） 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，應配合本公司辦理資訊安全訪視作業。
- （二） 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

- (三) 得標廠商應建立標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，除應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。
- (四) 得標廠商同意金融監督管理委員會、中央銀行、中央存款保險公司、農業部農業金融署等機關或依農業金融法第七條規定之機關及本公司或委託獨立第三方單位進行辦理本契約相關事項之稽核。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。
- (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。
- (六) 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。
- (七) 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。
- (八) 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。
- (九) 得標廠商因履行契約應辦事項所知悉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得標廠商員工，得標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得標廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。
- (十) 得標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）及經得標廠商之員工簽署之「保密同意書」至本公司備查，且對其操守行為負責。
- (十一) 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。
- (十二) 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。
- (十三) 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。

(十四) 得標廠商及分包商應擬定本契約項目之服務水準(SLA)：

1. 如無法訂定本契約項目之服務水準時，須擬定補償性控制措施。
2. 違反本公司資訊安全要求或因人員疏失等原因，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，得標廠商應與分包商依契約內容負連帶賠償責任。
3. 因本契約作業項目之性質、產品內容或服務，得標廠商無法提供服務水準或補償性控制措施時(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)，雙方之權利義務得依雙方協議內容另定之。

(十五) 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。
2. 得標廠商於契約履行期間，如得標廠商人員異動時(完成階段性任務或離職等情形)，得標廠商應會同委託單位將其借用之設備、軟體或其他物件返還予本公司，並移除相關作業權限。
3. 得標廠商不得任意複製或攜出本公司非對外公開之業務資料。本公司所提供之資訊資產及資料等，得標廠商均應於契約終止、解除或期限屆滿時返還予本公司，並刪除或銷毀因執行本契約而儲存持有之個人資料檔案，且不得以任何形式留存備份。得標廠商履行契約相關事務之資料處理流程及傳輸方式，應依本公司資料安全管控規定辦理。
4. 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。

(十六) 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。

(十七) 得標廠商所屬人員倘因參加本案系統建置、維護，致本公司蒙受損害，得標廠商應與其所屬人員負連帶賠償責任。

(十八) 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) 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。

(二十一) 得標廠商應依本公司業務需要，配合修改應用軟體之程式和文件。

(二十二) 得標廠商所提供之程式若有採用第三方套件(非得標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。

- (二十三)於專案建置或維護期間內，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，得標廠商應協助評估及處理，如係非得標廠商單方修正程式得以解決者(如需作業系統、資料庫、產品升級或原廠產品已終結等)，則不受前款規定限制，雙方得另議處理方法。
- (二十四)得標廠商所提供之程式及文件，無條件供本公司存查，惟不得公開予無關之第三者。於維護期間所開發應用程式與交付軟體，得標廠商應善盡義務執行資訊安全檢查是否內藏惡意程式，並出具相關資安檢測證明文件，本公司不另行付費。
- (二十五)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。
- (二十六)得標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，得標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)。
- (二十七)得標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，應由得標廠商負賠償責任。於契約履行期間得標廠商須配合本公司定期資安檢測作業或電腦資訊安全評估作業，例如弱點掃描、滲透測試、源碼檢測等，所檢測出之風險弱點項目，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。
- (二十八)得標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。
- (二十九)依前款規定之弱點檢測如因市場工具未能支援無法提出相關檢測文件，得標廠商應出具資訊安全聲明書。

三、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	企業網銀及個人網銀APP檢測服務(含iOS及Android) A. OWASP Top 10		1批	○○	○○○

	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				
二	取得行動應用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）。

四、 交貨、安裝及測試

- (一) 得標廠商須於簽約次日起8個月內完成網路銀行滲透測試及APP檢測並取得工業局證書。
- (二) 如逾前項所訂期限，得標廠商須依照下列公式計付違約金予本公司：

$$\text{違約金} = \text{契約總價款} \times 0.1\% \times \text{逾期日數}$$
 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。

五、 驗收與付款

- (一) 得標廠商於簽約次日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. 取得工業局證書 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

六、 維護及保固

得標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。

七、 得標廠商應提供本案相關教育訓練4小時及辦理技術移轉並詳列於工作說明書，本公司不另行付費。

八、 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。

附件 1

全國農業金庫股份有限公司委外廠商交付文件清單

填寫日期： 年 月 日

專案名稱			
委外廠商名稱		聯繫窗口	
地址		聯繫電話	
序號	交付項目	委外廠商提供佐證或說明	
1	列舉在本公司有效合約	<input type="checkbox"/> 已提供 <input type="checkbox"/> 未提供，說明：	
2	保密同意書、資訊安全聲明書、保證書、切結書	<input type="checkbox"/> 已提供 <input type="checkbox"/> 未提供，說明：	
3	本案所需工作計畫書或工作說明書(含專業能力與經驗)	<input type="checkbox"/> 已提供 <input type="checkbox"/> 未提供，說明：	
4	資訊安全通過第三方驗證之證明或驗證報告或有關之管理措施	<input type="checkbox"/> 已提供 <input type="checkbox"/> 未提供，說明：	

【備註事項】

1. 此評估表委外廠商應如實填寫，若經本公司審查後發現有填寫不實之情形，本公司得於通知委外廠商後終止或解除契約，因而致生之損害，委外廠商應負損害賠償責任。

委外廠商： (蓋章)

代表人： (蓋章)

日期：

全國農業金庫股份有限公司 保密同意書

- 一、立書人因承攬全國農業金庫股份有限公司（以下稱貴公司）
_____業務，茲承諾對於執行職務期間直接或間接所持有或知悉
之業務上資料或訊息，均願意遵守下列保密規定，絕不洩漏、交付予他人或
為不當目的之使用：
- （一）農業金融法第二十六條準用銀行法第四十八條第二項：「銀行對於顧客
之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定
者外，應保守秘密。」
- （二）農業金融法第二十六條準用銀行法第二十八條第四項：「銀行經營信託
及證券業務之人員，關於客戶之往來、交易資料，除其他法律或中央主
管機關另有規定者外，應保守秘密；對其他部門之人員，亦同。」
- （三）個人資料保護法對於個人資料之相關限制規定。
- （四）貴公司相關保密規定。
- 二、立書人如違反前述保密規定，除應負刑法第三百十七條：「依法令或契約有
守因業務知悉或持有工商秘密之義務而無故洩漏之者，處一年以下有期徒刑、
拘役或三萬元以下罰金。」之刑責外，並願負一切法律上責任，如因而致貴
公司遭受損害，並願負擔損害賠償責任，包含委託契約所負擔賠償責任，絕
無異議。

此致

全國農業金庫股份有限公司

立書人：

代表人：

統一編號：

地 址：

中 華 民 國 年 月 日

全國農業金庫股份有限公司 資訊安全聲明書

公司(以下稱本公司)因承攬全國農業金庫股份有限公司(以下稱貴公司)採購案(契約編號：)所提供之程式與軟體(含套裝軟體)，本公司將善盡義務執行資訊安全檢查，執行安全性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)，且善盡檢查應用程式與軟體安全管理與資訊安全環境維護責任，若因本公司違反造成貴公司或第三者之直接實際損害，本公司將負擔民事、刑事責任，包括因此所致貴公司涉訟所須支付之訴訟費用或對第三人賠償之金額，並於第三人對貴公司提出請求、訴訟，經貴公司以書面通知本公司提供相關資料，本公司應合作提供，絕無異議。

此致

全國農業金庫股份有限公司

立書人：

代表人：

統一編號：

地 址：

中 華 民 國 年 月 日

全國農業金庫股份有限公司 保證書

立書人_____（以下稱本公司）因承攬全國農業金庫股份有限公司（以下稱貴公司）_____業務，本公司保證日後倘有因本公司所屬人員或所委託人員因素致貴公司蒙受損害，本公司願負連帶賠償責任。

此致

全國農業金庫股份有限公司

立書人：

代表人：

統一編號：

地 址：

中 華 民 國 年 月 日

全國農業金庫股份有限公司 切結書

立書人 _____ 公司（以下稱本公司）因承攬全國農業金庫股份有限公司（以下稱貴公司）_____業務，切結如下：

- 一、 辦理貴公司本標案，本公司專案團隊（含分包廠商）於契約範圍內提供使用之資通訊產品（含軟體、硬體及服務），包含用以設計、開發、維護及管理契約標的等、個人或公司連接至貴公司內部網路或設備者，均無提供使用中國廠牌資通訊產品及資通訊服務。
- 二、 本公司茲切結於投標時並無違反前項之情事；並承諾於契約期間內，本公司專案團隊（含分包廠商）亦絕不提供使用中國廠牌資通訊產品及資通訊服務，且同意遵守主管機關及貴公司有關資訊安全之規範及要求。如有違反任一切結及承諾事項致貴公司受有損害，願承擔相關法律責任並負賠償責任。

此致

全國農業金庫股份有限公司

立書人：

代表人：

中 華 民 國 年 月 日

全國農業金庫股份有限公司委外廠商安全評估表

專案名稱					
委外廠商名稱					
序號	評估項目	評定結果			
1	委外廠商於本公司並無服務集中度過高之情形	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合，說明：			
2	委外廠商已簽署保密同意書、資訊安全聲明書、保證書、切結書	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合，說明：			
3	委外廠商已提供本案所需工作計畫書或工作說明書(含專業能力與經驗)	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合，說明：			
4	委外廠商已提供通過第三方驗證之證明或驗證報告或有關之管理措施	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合，說明：			
		經辦	襄理	副理	主管
業務需求單位					
資訊安全部		綜合以上說明， <input type="checkbox"/> 符合 <input type="checkbox"/> 不符合，說明：			
		經辦	襄理	副理	主管

全國農業金庫股份有限公司 保密同意書

- 一、立書人任職或受雇於_____公司（以下稱本公司），本公司因承攬全國農業金庫股份有限公司（以下稱貴公司）_____業務，茲承諾對於執行職務期間直接或間接所持有或知悉之業務上資料或訊息，均願意遵守下列保密規定，絕不洩漏、交付予他人或為不當目的之使用：
- （一）農業金融法第二十六條準用銀行法第四十八條第二項：「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密。」
- （二）農業金融法第二十六條準用銀行法第二十八條第四項：「銀行經營信託及證券業務之人員，關於客戶之往來、交易資料，除其他法律或中央主管機關另有規定者外，應保守秘密；對其他部門之人員，亦同。」
- （三）個人資料保護法對於個人資料之相關限制規定。
- （四）貴公司相關保密規定。
- 二、立書人如違反前述保密規定，除應負刑法第三百十七條：「依法令或契約有守因業務知悉或持有工商秘密之義務而無故洩漏之者，處一年以下有期徒刑、拘役或三萬元以下罰金。」之刑責外，並願負一切法律上責任，如因而致貴公司遭受損害，並願負擔損害賠償責任，包含委託契約所負擔賠償責任，絕無異議。

此致

全國農業金庫股份有限公司

立書人：

身分證統一編號：

地 址：

中 華 民 國 年 月 日

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規範，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。