

全國農業金庫風險導向內部稽核系統規格及特別條款

全國農業金庫股份有限公司(以下稱本公司)採購「風險導向內部稽核制度專案」(以下稱本案)，其規格及特別條款規定如下：

甲、規格

壹、服務規格

項次	工作內容	交付項目
(一)	稽核作業系統	
	建置包括下列功能之系統： <ol style="list-style-type: none"> 稽核作業基本資料 <ul style="list-style-type: none"> 主管覆核 基本資料設定 稽核題庫 <ul style="list-style-type: none"> 維護流程 維護風險 維護控制點 稽核規劃 <ul style="list-style-type: none"> 分派題目 分派人員 分配題目 實地稽核 <ul style="list-style-type: none"> 建立稽核報告 內外部稽核缺失複查 外部稽核缺失追蹤(媒體檔案上傳外檢缺失) 	交付項目： <ol style="list-style-type: none"> 測試報告 系統架構書 資料庫檔案說明書 程式規格書 使用者操作手冊 備援作業程序書 原碼檢測報告 弱點掃描報告
(二)	稽核作業精進流程方法論	
	<ol style="list-style-type: none"> 風險導向內部稽核技術方法論說明(8小時) 教育訓練(8小時)含會議及實務討論 	交付項目： <ol style="list-style-type: none"> 稽核作業精進流程方法論報告 會議簽到表
(三)	建置銀行內部稽核風險評估程序	
	建置內部稽核風險評估方法： <ol style="list-style-type: none"> 決定內部稽核之受查主體 	交付項目： 經營風險類型範本、監控指標會議記錄、固

	2. 評估受查主體的固有風險等級、控制措施有效性以及剩餘風險等級 3. 規劃受查主體的風險監控指標	有風險評估細項範本
(四)	風險評估系統	
	建置包括下列功能之系統： <ol style="list-style-type: none"> 1. 風險評估基本資料 2. 風險評估 3. 稽核品質評核 4. 主管覆核 5. 風險評估結果查詢 	交付項目： <ol style="list-style-type: none"> 1. 測試報告 2. 系統架構書 3. 資料庫檔案說明書 4. 程式規格書 5. 使用者操作手冊 6. 備援作業程序書 7. 原碼檢測報告 8. 弱點掃描報告
(五)	輔導申請「風險導向內部稽核」資格（含相關申請文件）	
	提供向主管機關申請「風險導向內部稽核資格」資格文件範本，並依據現況協助修訂： <ol style="list-style-type: none"> 1. 內部控制三道防線實務守則 2. 偵測經營風險之內部規範 3. 風險導向內部稽核制度規範 4. 內部稽核品質評核機制 	交付項目： <ol style="list-style-type: none"> 1. 申請風險導向內部稽核資格文件範本

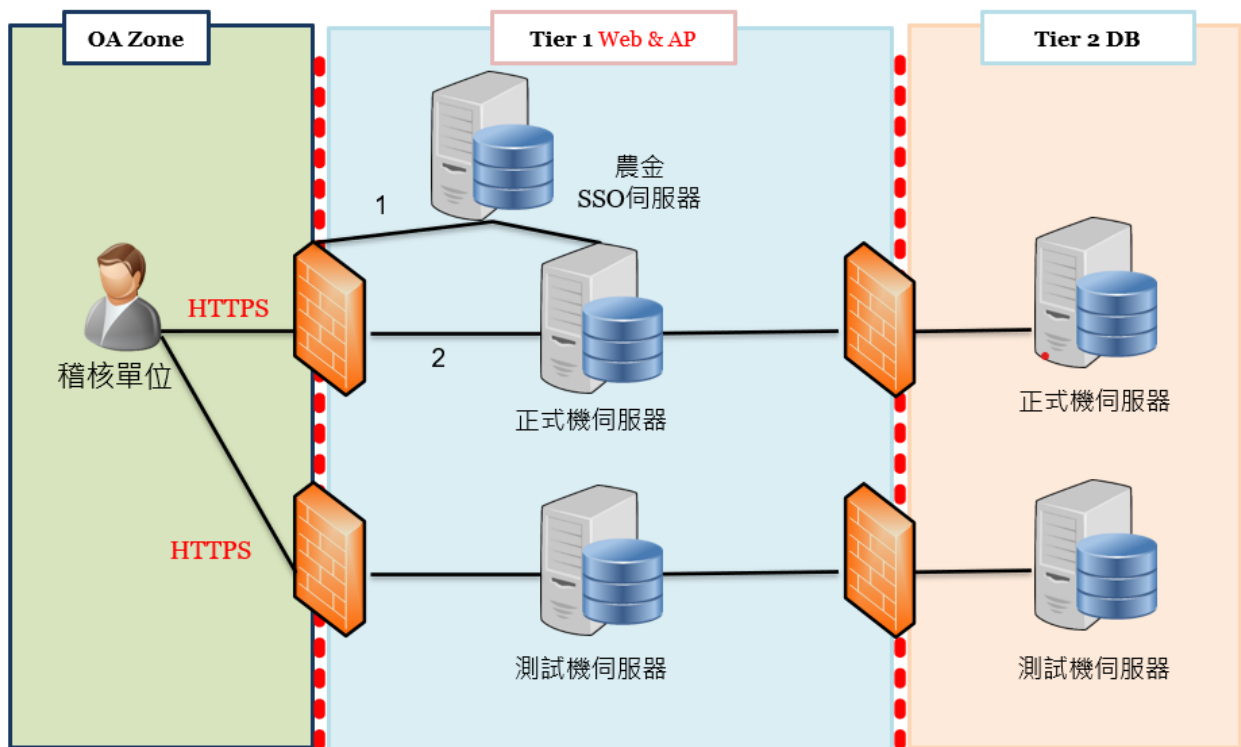
貳、系統規格

- 一、 本案設備需安裝於本公司指定地點並完成所要求之設定、調整及測試。
- 二、 本案設備應配合本公司現有備份模式，進行系統備份作業。
- 三、 本案廠商須提供正式、開發測試作業環境建置建議，並配置所需之開發工具、系統軟體（不合作業系統、MS SQL，其所需數量由本案廠商提供建議，由本公司採購）、應用軟體等足夠合法使用版權數，本公司不另行付費。
- 四、 本案設備應符合本公司現行軟硬設備規劃（建置在 VMWare 系統上 Windows Server 及 MS SQL Server）。
- 五、 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 條第 1 項第 1 款、第 2 款之規定，於 3 年或 1 年期限內，不得參加議價或作為議價對象或分包廠商。
- 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、郵政匯票繳納押標金，得標後押標金轉為履約保證金，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，未得標者無息退還。

七、 本規格稱 " 以上" 、" 以下" 、" 以內" 、" 至少" 、" 高於" 、" 低於" 俱含本數。

八、系統架構圖



1. 透過 SSO 連線

2. 透過獨立登入頁面連線(備用)

九、硬體設備規格

1. 正式環境共 2 臺

- (1) 中央處理器：2 核心以上
- (2) 主記憶體：32GB 以上
- (3) 硬碟空間：500GB 以上

2. 測試環境共 2 臺

- (1) 中央處理器：2 核心以上
- (2) 主記憶體：16GB 以上
- (3) 硬碟空間：300GB 以上

十、系統軟體規格

1. 正式環境及備援環境

- (1) Windows Server 2019 以上伺服器企業中文版作業系統 1 套
- (2) Microsoft SQL Server 2016 以上標準版資料庫 1 套

2. 測試環境

- (1) Windows Server 2019 以上伺服器企業中文版作業系統 1 套
- (2) Microsoft SQL Server 2016 以上標準版資料庫 1 套

參、 功能需求

詳附件-「風險導向內部稽核系統功能需求」。

乙、 特別條款

壹、 本案設備維護工作應由本案廠商承擔。

貳、 本案廠商對於本案設備同意履行以下二十二款情事：

- 一、 為應外規異動需要，本案廠商對於所開發之應用軟體須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、 本公司如因外規異動需要對本案廠商所提供之程式或文件得作適當之修改。
- 三、 本案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需另案處理。
- 四、 本案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，本案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。
- 五、 本案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，應由本案廠商負賠償責任，於維護期間本案廠商須配合本公司定期資安檢測作業(如:弱點掃描、滲透測試、原碼檢測等)，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。
- 六、 本案廠商提供本公司使用之軟體，如有第三者主張本案廠商所提供本公司使用該軟體有侵犯專利權或著作權時，本公司同意儘速以書面通知本案廠商，本案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）、所受之損害等均由本案廠商負擔。
- 七、 本案廠商應訂定其聘僱人員之相關管理規定，並將開發及維護（修）人員名冊（含簽章）函送本公司備查，且對其操守行為負責，如有異動時亦同。
- 八、 本案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之相關資料及內容，應採取必要之安全措施，本案廠商及其員工均應保守秘密不得洩漏，否則如致本公司遭受損害應由本案廠商負賠償責任；契約終止時亦同。
- 九、 本案廠商因履行契約應辦事項所應負之損害賠償責任以直接實際損害為限，且以契約總價款為賠償上限。但有關人身傷害（包含死亡）、物之毀損、專利權及著作權之損害、本案廠商之故意或重大過失造成之損害賠償則不在此限。

- 十、 本案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、行政院農業委員會農業金融局或依農業金融法第七條規定之機關及本公司得取得契約應辦事項相關資料或報告，及進行金融檢查或稽核，或得要求其於期限內提供相關資料或報告。
- 十一、 本案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。
- 十二、 本案廠商應依本公司同意之標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度。契約如有履行不能、履行困難或履行困難之虞者，本案廠商應即通知本公司。
- 十三、 本案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。
- 十四、 本案廠商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。
- 十五、 本案廠商非經本公司事先書面同意，不得將契約應辦事項複委託。
- 十六、 本案廠商對契約應辦事項若有重大異常或缺失應立即通知本公司。
- 十七、 本案廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知本案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。
- 十八、 本案廠商對於所開發之應用軟體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：應用程式應於上線前通過原碼檢測、系統應於上線前通過弱點掃描、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。
- 十九、 上述弱點檢測如因市場工具未能支援無法提出相關檢測文件，本案廠商應出具「委外開發應用程式與軟體-資訊安全聲明書」（如附件）。
- 二十、 本案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；於維護期間內若採用之第三方套件有公開風險揭露，須配合本公司於期限內修正，本公司不另付費。
- 二十一、 於專案維護期間內，為解決第三方套件有公開風險揭露之修正，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。

二十二、本案廠商須符合本公司現有各項系統管理作業規定及安全管理規範。

肆、報價

本案廠商以新臺幣為報價基礎，且分別依下表列出價格： 單位：元

項次	品名	數量	單價	金額
一	稽核作業系統	1式	000	000
二	稽核作業精進流程方法論	1式	000	000
三	建置銀行內部稽核風險評估程序與方法	1式	000	000
四	風險評估系統功能	1式	000	000
五	輔導申請「風險導向內部稽核」資格(含相關申請文件)	1式	000	000
合計				000

*以上報價應依規格內容報價(含稅)。

伍、交貨、安裝及測試

一、本案廠商須於簽約次日起 4 個月內交付經本公司簽認之工作說明書與需求規格說明書，如逾所訂期限，本案廠商須依照下列公式計付違約金予本公司：

$$\text{違約金} = \text{契約總價款} \times 0.1\% \times \text{逾期天數}$$

二、本案廠商需於簽約次日起 9 個月內完成本案第一階段稽核系統之開發及測試並提出經本公司簽認之測試報告，如逾所訂期限，本案廠商須依照下列公式計付違約金予本公司：

$$\text{違約金} = \text{契約總價款} \times 0.1\% \times \text{逾期天數}$$

三、本案應於簽約次日起 36 個月內完成所有階段文件交付。若有其他不可抗外力、功能需求變更或新增服務等，時程順延期間則由雙方另行議訂。

四、上述作業，如逾期超過 30 天仍未完成時，除仍應依上述規定計付違約金外，本公司得通知解除契約，並沒入履約保證金。

五、上開違約金總額以契約價款之 20%為上限。

陸、驗收及付款

本案廠商交付相關文件後，由本公司辦理驗收，驗收合格後，分階段支付各期款項，各階段支付款項及應交付相關文件如下：

階段	工作內容	交付項目及文件	支付款項
簽約	完成簽約作業並交付合約正本時		契約總價款 16%

第一階段	稽核作業系統：完成系統建置，包括下列功能之系統： 1. 系統設定 2. 維護稽核作業題庫流程 3. 維護稽核作業基本資料流程 4. 實地稽核作業流程	1. 測試報告 2. 系統架構書 3. 資料庫檔案說明書 4. 程式規格書 5. 使用者操作手冊 6. 備援作業程序書 7. 原碼檢測報告 8. 弱點掃描報告	契約總價款 23%
第二階段	稽核作業精進流程方法論： 1. 風險導向內部稽核技術方法論說明(8小時) 2. 教育訓練(8小時)含會議及實務討論	1. 稽核作業精進流程方法論報告 2. 會議簽到表	契約總價款 2%
第三階段	召開專案啟動會議_與業管部門	業管專案啟動會議記錄	契約總價款 8%
	建置銀行內部稽核風險評估程序與方法： 1. 決定內部稽核之受查主體 2. 評估受查主體的固有風險等級、控制措施有效性以及剩餘風險等級 3. 規劃受查主體的風險監控指標	1. 經營風險類型範本 2. 監控指標會議記錄 3. 固有風險評估細項範本	契約總價款 8%
第四階段	召開稽核風險評估系統專案啟動會議	專案啟動會議記錄	契約總價款 8%
	稽核風險評估系統：建置包括下列功能之系統： 1. 風險評估基本資料 2. 風險評估 3. 稽核品質評核 4. 主管覆核 5. 風險評估結果查詢	1. 測試報告 2. 使用者操作手冊 3. 教育訓練講義	契約總價款 18%
第五階段	輔導申請「風險導向內部稽核」資格(含相關申請文件)： 提供向主管機關申請「風險導向內部稽核資格」資格文件範本，並依據現況協助修訂：	申請風險導向內部稽核資料文件範本	契約總價款 8%
	1. 內部控制三道防線實務守則 2. 偵測經營風險之內部規範 3. 風險導向內部稽核制度規範 4. 內部稽核品質評核機制	申報文件已送至主管機關時	契約總價款 9%

柒、 維護及保固

- 一、 本案廠商必須提供維護本案設備之技術工程師週一至週五上班日待命維修之服務，以維護本案設備之正常運作，如於非上班日遇有設備損壞需更換零件之情事，則最遲須於次一上班日完成維修恢復運作。
- 二、 本案廠商對於其所提供之本案設備，於本案完成全案驗收之次日起，負責維護及保固 1 年，不另行付費；保固期滿後，本公司得視實際需要與本案廠商簽訂維護契約，其每年維護費率為契約總價款之 8%，本案廠商不得拒絕簽約，若本公司要求簽訂維護契約而本案廠商未於保固期間屆滿前與本公司簽訂維護契約，則保固期自動延長至維護契約生效日止。
- 三、 維護期間交付應用程式過版時，本案廠商須檢附程式原碼檢測報告或資安相關檢測證明，確認完成後，才允進行應用程式過版作業，本公司不另行付費。

捌、 本案廠商應依本公司電腦及資訊作業安全之相關規定建置安控作業環境及作業流程。

玖、 本案廠商應提供本案相關教育訓練至少 4 小時並辦理技術移轉，本公司不另行付費。

壹拾、 本案廠商應對本案契約內容充分瞭解，並依本公司之解釋切實執行辦理。

附件

風險導向內部稽核系統功能需求

壹、內部稽核作業系統：

系統功能類別	功能名稱	說明
一、系統設定	維護功能群組	設定各類角色清單與其擁有之功能權限
	維護使用者	設定使用者帳號清單與其角色
	稽核軌跡查詢	可設定條件，查詢各使用者使用本系統之紀錄
	維護指標群組關係矩陣	可上傳檔案以批次設定各風險監控指標，監控之權重群組清單
二、維護稽核作業題庫流程	維護流程	1. 維護流程與次流程無須進行覆核。 2. 透過畫面新增、修改、刪除主流程，次流程。
	維護風險	1. 維護風險無須進行覆核。 2. 透過畫面新增、修改、刪除風險描述及風險類型。
	維護控制點	1. 維護控制點是在覆核題庫做覆核 2. 透過畫面新增、修改、刪除控制點描述，選擇受查主體及相對應的業務類型。
三、維護稽核作業基本資料流程	維護控制點標籤	透過畫面新增、修改、刪除控制點標籤。
	維護業務類型	透過畫面新增、修改、刪除業務類型。
	維護查核類型	透過畫面新增、修改、刪除查核類型。
	維護稽核發現等級	透過畫面新增、修改、刪除稽核發現等級
	維護稽核報告等級	透過畫面新增、修改、刪除稽核報告等級
	維護建議樣本量	透過畫面修改建議樣本量
	維護稽核組別人員	透過畫面新增、修改、刪除稽核組別

系統功能類別	功能名稱	說明
	維護稽核科別人員	透過畫面新增、修改、刪除稽核科別
四、 實地稽核 作業流程	建立年度稽核作業	引用風險評估期別資訊建立年度稽核作業期別
	指派受查主體含題目	可依照風險類型、查核類型、以及指定控制點的方式進行分派作業，將題目與該次分派的受查主體進行連結。或分派尚未送交主管覆核，可以通過此功能進行刪除。
	刪除指派受查主體含題目	若已通過覆核的分派，需要通過此功能進行刪除。
	指派稽核人員	針對該次分派作業，可於此功能指派對應的領隊稽核以及查核人員。
	分配題目	決定了受查主體題目以及指派稽核人員後，可以將題目分配與稽核人員。
	實地稽核	可針對控制點之執行有效性、設計有效性進行查核，並根據查核發現開立稽核發現
	覆核實地稽核	針對〈實地稽核〉送審之內容進行審核。
	實地稽核初審	實地稽核步驟中〈設計有效性〉、〈執行有效性〉除了有效性狀態為〈有效〉之外的狀態都是稽核發現有問題，以及〈開立稽核發現〉在覆核實地稽核後還需要再送交〈實地稽核初審〉
	建立稽核彙總	當整個實地稽核作業完成時，可透過此功能檢視控制點完成進度，以及所開立的稽核發現內容，進一步針對整體資料進行彙總說明。
	覆核稽核彙總	針對〈建立稽核彙總〉內容進行覆核。
	轉出稽核缺失	可單獨匯出實地稽核建立之稽核發現內容

貳、風險評估系統：

系統功能類別	功能名稱	說明
一、	維護權重群	可依期別(註解(1))設定權重群組，並送交主管覆核

系統功能類別	功能名稱	說明
風險評估 基本資料	組	設定功能包含新增、修改、刪除
	維護查核群組	可依期別設定查核群組，並送交主管覆核 設定功能包含新增、修改、刪除
	維護受查主體	可依期別設定受查主體，並送交主管覆核 設定功能包含新增、修改、刪除
	維護經營風險	可依期別設定經營風險，並送交主管覆核 設定功能包含新增、修改、刪除
	維護風險權數	可依期別設定各權重群組之經營風險權數，並送交主管覆核
	維護控制措施權數	可依期別設定各權重群組之控制措施權數，並送交主管覆核
	維護監控指標	可依期別設定監控指標，並送交主管覆核 設定功能包含新增、修改、刪除
	維護控制措施細項	可依期別設定控制措施細項，並送交主管覆核 設定功能包含新增、修改、刪除
	維護查核頻率設定	可依期別檢視並設定各查核群組風險等級高、中、低時，一般與專案的查核頻率，並送交主管覆核
二、 風險評估	建立風險評估期別	可建立期別並送交主管覆核
	上傳風險評估資料	可依期別上傳風險評估檔案，包含固有風險評估檔案(註解(2))、風險紀錄簿(註解(3))及控制措施有效性評估檔案(註解(4))
	計算剩餘風險	可依期別根據上傳之風險評估資料，設定計算之相關參數，並進行剩餘風險之計算
	調整剩餘風險	可依期別於剩餘風險計算之後，依特殊情形調整特定受查主體之剩餘風險，並送交主管覆核
	確認風險評估結果	確認任一期別已評估完成且不會再有任何資料變更，可送交主管覆核後結案
三、 稽核品質 評核	設定品質評核內容	可根據法規規定項目，設定品質評核之細項及重點題目
	內稽品質評核	可根據品質評核內容，於自選季度實際進行內稽品質評核，並將評核結果送交主管覆核
	品質評核意見追蹤	可搜尋已建立之內稽品質評核結果，並追蹤品質評核缺失改善情形
	品質評核結果查詢	可查詢品質評核結果
四、 主管覆核	覆核風險評估期別	由主管覆核【建立風險評估期別】之請求
	覆核風險評估基本資料	由主管覆核【風險評估基本資料】各功能之新增/修改/刪除請求

系統功能類別	功能名稱	說明
	覆核調整剩餘風險	由主管覆核【調整剩餘風險】之請求
	覆核風險評估結果	由主管覆核【確認風險評估結果】之請求
	覆核品質評核	由主管覆核【內稽品質評核】之請求
	覆核使用者權限	由主管覆核【維護功能群組】與【維護使用者】之請求，並可查詢功能群組與使用者權限變動之申請與覆核軌跡
五、風險評估結果查詢	全部主體剩餘風險	可依期別於【計算剩餘風險】執行計算完畢後，查詢該期別所有受查主體之風險評估結果，並可將結果下載為 Excel 檔案
	單一主體剩餘風險	可依期別於【計算剩餘風險】執行計算完畢後，查詢該期別單一受查主體之風險評估結果細項，並可將結果下載為 Excel 檔案
	多期比較剩餘風險	可以設定任一已計算出剩餘風險之期別為基期，與後續評估期別間之受查主體綜合風險評估結果比較差異，並可將比較結果下載為 Excel 檔案
	檢視稽核計畫	可上傳針對所有受查主體之查核計畫資料，由系統比對查核計畫符合查核頻率設定之情形
	風險評估資料上傳進度查詢	可依期別檢視【上傳風險評估資料】檔案上傳情形

參、採購管理系統之功能需求除上列各項外，本案廠商於需求訪談後交付之需求規格說明書亦為功能需求之一部。

肆、系統架構為 Web 架構，並以 Java 作為系統開發框架。

附件

委外開發應用程式與軟體-資訊安全聲明書

茲_____ (下稱本公司) 因承攬 貴公司「風險導向內部稽核制度」採購案(案號: _____) 所開發應用程式與軟體, 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、間諜軟體等)及隱密通道(Tunnel channel), 且於交付時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

立聲明書人

公司名稱:

負責人:

統一編號:

地址:

中 華 民 國 年 月 日