

全國農業金庫資訊安全委外監控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）採購「資訊安全委外監控服務」（以下稱本案服務），其規格及特別條款規定如下：

甲、規格

壹、一般規定：

- 一、投標廠商應提供使用軟體之原廠所開立合法授權使用證明書影本。
- 二、投標廠商於投標截止日近3年內，應具備3家以上金融機構(銀行業、證券業及保險業)或依金管會公告金融周邊機構之相關資訊安全委外監控服務經驗，提供採購契約、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無息發還，未得標者無息退還押標金。
- 四、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
- 五、本規格稱"以上"、"以下"、"以內"、"至少"、"高於"、"低於" 俱含本數。

貳、本案服務地點、收容監控標的清單規格、服務項目：

(一) 服務地點：

本公司資訊安全部:臺北市中正區館前路77號11樓。

本公司板橋機房:新北市板橋區縣民大道一段291號7樓。

(二) 收容監控標的清單規格：

項次	設備類型	廠牌	型號	數量
1	WAF	iMperva	SecureSphere X2530 WAF/500M HTTP throughput	1
2	Firewall	Fortinet	Internal : FG800D	1
		Paloalto	DMZ : PA850B	1
3	IPS	Radware	DefensePro X10	1
4	AD	Windows	Windows	2
5	L7 防火牆	Forcepoint	TRITON AP-WEB, With Web	1

			Hybrid Module, With Web DLP Module	
6	APT	Trendmicro	Deep Discovery Inspector	1
7	Antivirus	Symantec	Symantec endpoint protection manager	1
8	swift 主機	Windows 平台	AP xml log	1
			OS security event log	1
9	檔案伺服器	Windows 平台	Windows	1
10	白名單管控設備	Trendmicro	Safelock	1
11	Mail gateway	Symantec	Symantec Message Gateway	1
12	網站 IIS Log	Windows 平台	Windows IIS	2
13	公文電子系統交換主機	Windows 平台	AP log	1
			OS security event log	1
14	VPN 主機	Pulse Security	PSA 7000	1
15	DB Auditor	iMperva	V4500	1
16	MDR	Sentinel one	MDR Manager portal	1
17	Deep Security	TrendMicro	Deep Security Manager	1
18	DDEI	TrendMicro	DDEI Manager	1
19	MDM	Ivanti	Endpoint Manager Mobile	1
20	NDR	ExtraHop	ExtraHop Manager	1

(三) 服務項目：

項次	項目/內容	數量
1	SOC 資安預警監控服務，訂閱服務一年。 1. 日誌收集器主機收集軟體維護。 2. 7x24 資安監控通報:郵件/簡訊/電話。 3. 全球資安預警情報:惡意中繼站/網域清單。 4. 資安事件網頁管理與登入帳號。 5. F-SOC 資安聯防暨自動化情資分享作業。 6. 資安事故鑑識調查服務。 7. 資料保存並提供查閱，提供服務停止日起往前推算 1 年收容至 SOC 中心 log 備份；配合主管機關稽核作業，協助調閱資料。	1 年
2	提供本公司年度資安教育訓練教材及影音檔。 1. 一般資安通識教育訓練 3 小時(內容應包含隱私保護個資管理及社交工程防範)。	1 式

	2. 一般使用者暨管理者物聯網教育訓練 1.5 小時。	
3	SOC 專業顧問定期諮詢服務一年 1. 每月到府簡報前月資安事件分析。 2. 每季到府簡報，提供本公司安全防禦趨勢與最新資安訊息。	1 年

乙、特別條款

壹、 本案廠商同意履行以下事項：

- 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。本案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、 本案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、 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、 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、 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，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，本案廠商應立即以口頭、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. 本案廠商因履行契約應辦事項所知悉或存放於本案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本案廠商員工，本案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本案廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。
2. 本案廠商於契約履行期間應提供本案廠商服務人員名冊（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、本案廠商提供本公司使用之軟硬體應為合法，如有第三者主張本案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。

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），本案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、本案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；本案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，本案廠商應與分包商負連帶損害賠償責任。

十二、本案廠商資訊安全責任：

1. 本案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，此外本公司保有對本案廠商執行稽核權利，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，或由本案廠商提供公正第三方之驗證報告。

2. 本案廠商於契約經終止、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），本案廠商應完成本公司資訊資產與資料返還、移交、刪除或銷毀，並移除本案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. 本案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. 本案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、本案廠商組織重大調整、業務重大異動或契約提前終止等；如本案廠商服務內容異動對資訊安全有所衝擊，本案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. 因本案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，本案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、本案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、本案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、本案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、本案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、本案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、本案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，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、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、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廠商所提供之程式或文件得作適當之修改。
- 二十三、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。
- 二十四、因可歸責於本案廠商而終止契約，本公司得要求本案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，本案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，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。

貳、報價

本案服務以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	項目/內容	數量	單位	單價	金額
1	SOC 資安預警監控服務，訂閱服務 1 年	1	年	000	000
2	提供本公司年度資安教育	1	式	000	000

	訓練教材及影音檔				
3	SOC 專業顧問定期諮詢服務 1 年	1	年	000	000
合計					000

*以上報價應依規格內容報價(含稅)。

參、交貨

- 一、本案廠商須於簽約次日起2個月內，交付肆-二應交付相關文件，如逾所訂期限，本案廠商應依照下列公式計付懲罰性違約金予本公司：

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

- 二、如逾期超過1個月仍未完成交貨時，除仍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，並沒入履約保證金，且不補償廠商所生之損失。
- 三、上開逾期懲罰性違約金之累計總額以契約總價款之20%為上限，並得自契約總價、履約保證金中扣抵。
- 四、本案訂閱服務及顧問諮詢服務期間為1年。服務起始日以雙方實際訂閱日為準，服務迄日依實際起始日起算順延1年。

肆、驗收與付款

- 一、本案廠商依約交付相關文件後，提出經本公司簽認之交貨簽認單，由本公司派員辦理驗收，驗收合格後，支付契約總價款之 50%；其餘價款，由本案廠商依訂閱服務起算日起，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 25%，按期付款，共 2 期。

二、應交付相關文件如下：

1. 收容監控標的(即甲、規格-貳-(二)項次 1 至項次 20)收容完成證明書。
2. SOC 資安預警監控服務訂閱證明書。
3. 教育訓練教材及影音檔光碟(包含一般資安通識教育訓練3小時、一般使用者暨管理者物聯網教育訓練1.5小時)。

- 伍、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。

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	技術支援服務時間規定為本公司之營業日(上午 9 點至下午 6 點)，若因國定假日異動則以公告為準。
	3	服務中斷	服務期間內，若對於資安事件的發生，資安監控系統(以下均係指本案廠商之監控系統)無法於 4 小時內恢復系統運作至正常狀況，每逾 24 小時(含例假日與其他休息日)按契約總價之 0.1%計算懲罰性違約金，並由履約保證金逕行扣除，惟若屬本公司硬體設備或電路問題，則不在此限。 服務期間內資安監控系統累計當機總次數超過 5 次或當機總時數超過 52 小時後，自第 6 次當機或第 52 小時起(含)，每當機一次或每逾 4 小時，按契約總價之 0.1%計算懲罰性違約金，並由履約保證金逕行扣除。
	4	問題回應時間	接獲本公司通知後(含電話、簡訊、E-Mail、傳真、書面或其他通訊軟體等)，須於通報後 5 日內回應，一般處理時間不應超過收件後隔日起算 10 日，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 3 日內到場服務。
	5	復原點目標	發生故障時，將 VM 故障點之服務狀態還原至其他虛擬主機繼續提供服務。

二、相關說明：

- (一) 本案廠商違反資訊安全與服務水準時，如需延長日期或非本案廠商之問題(不納入計罰)，須經本公司同意。
- (二) 本案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) 本案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) 本案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) 如懲罰性違約金總額達契約總價之 20%時，本公司得通知本案廠商終止契約或解除契約之部分或全部，且不補償本案廠商所生之損失。
- (六) 本案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。