工業技術研究院
資通系統委外資安要求文件

版本日期：2026/06/15

購案名稱：

[　LSMS 系統優化、滿意度問卷電子化　]

請再次確認您此次購案的標的網站，其計畫(需求或需求)來源為執行政府計畫或本院自身業務推動，如果計畫(或需求)來源為民間廠商，則不在本院資通委外管理範圍，請回請購單勾選「否」，以免耽誤您的購案後續時程。

填寫需知：請下載填寫說明，本表單填寫如有任何問題，請聯繫資通安全管理法推動小組 cybersecurity@itri.org.tw 或資訊處服務窗口 18899，謝謝。

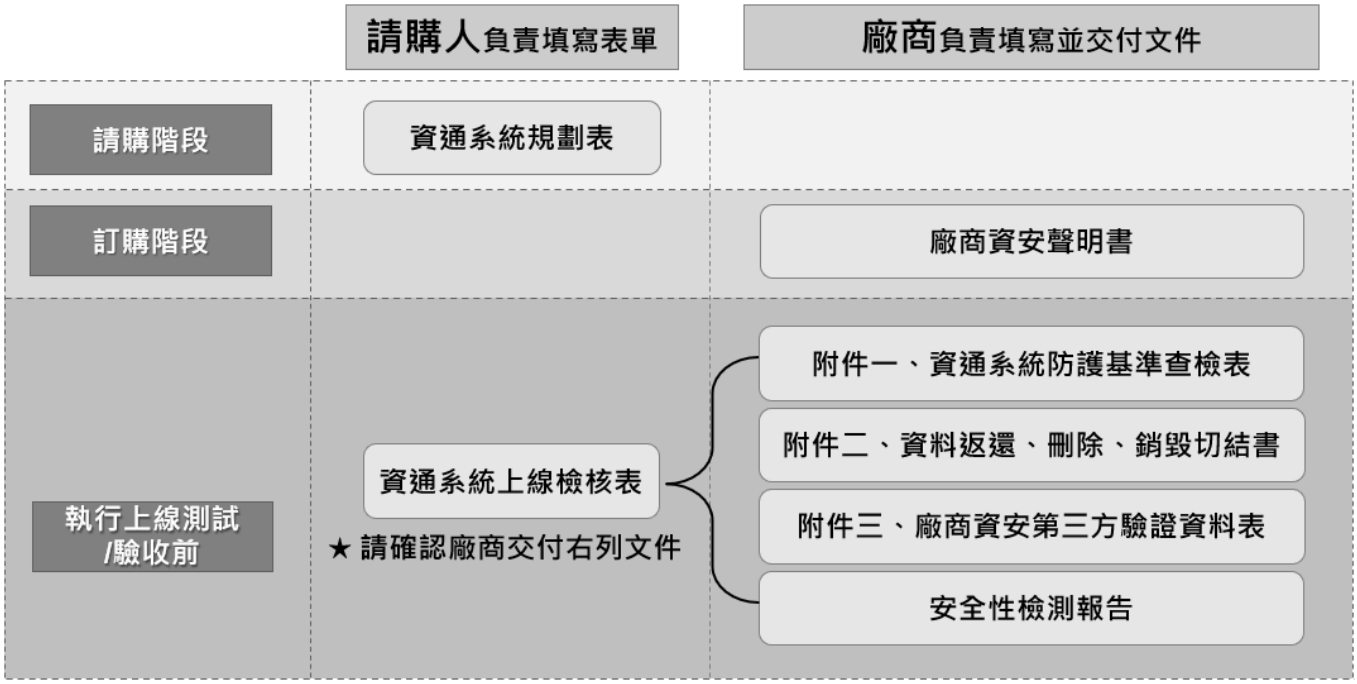
本檔案中包含以下文件：

文件名稱	負責填寫人	文件填寫時間點
資通系統規劃表	請購部門	請購階段
廠商資安聲明書	委外廠商	訂購階段
資通系統上線檢核表	請購部門	執行上線測試時或驗收前
附件一、資通系統防護基準查檢表	委外廠商	執行上線測試時或驗收前
附件二、資料返還、刪除、銷毀切結書	委外廠商	執行上線測試時或驗收前
附件三、廠商資安第三方驗證資料表	委外廠商	執行上線測試時或驗收前

工業技術研究院
Industrial Technology
Research Institute

文　件　填　寫　指　引

依據《工業技術研究院資訊作業委外安全管理準則》之規範，請購部門與委外廠商需於請購案各階段完成指定文件，以確保資訊安全並降低委外作業所帶來的之資安風險。請購人請依本指引逐步完成文件填寫與確認，確保採購案順利進行並符合院內資安要求。



一、 請購階段

由請購部門填妥「資通系統規劃表」後上傳至請購單，系統將自動加簽單位資推委員核定。

二、 採購階段

由採購同仁提供「廠商資安聲明書」與附件表單予廠商，此階段廠商需回簽「廠商資安聲明書」供本院留存。

三、 執行上線測試/驗收前

請購部門應於執行資通系統上線測試時或驗收前，填寫「資通系統上線檢核表」，並確認廠商已交付以下文件：

- 附件一、資通系統防護基準查檢表
- 附件二、資料返還、刪除、銷毀切結書
- 附件三、廠商資安第三方驗證資料表(*註)
- 安全性檢測報告

以上資料由請購部門自行留存，以備主管機關查核需要。

*註：本廠商如未通過資安第三方驗證，於驗收交付時須提供以商用軟體執行程式碼源碼掃描或滲透測試報告，並修補至無高風險。

工業技術研究院
Industrial Technology Research Institute

資 通 系 統 規 劃 表

請購部門
開立購案前
填寫

為協助全院各單位辦理資通委外案件落實資通安全管理法(及子法)與主管機關之要求(如資通系統籌獲各階段資安強化措施)，訂定本表，請購部門開立請購單前完成填寫，上傳至請購申請單後，系統自動加簽單位資推委員確認以下內容，即可辦理資通委外。

一、有關本購案委外開發之資通系統的資通系統防護需求分級為□普 ■中 □高，請檢附審查紀錄或填寫下表評估表。

■是 □否 已於本院本院對外網站暨數位平台應用登錄及管理系統登錄。資通系統名稱為： 工研院產業學習網報名系統

□是 ■否 為政府委辦計畫契約要求的資通系統。

選「是」者免填下表，應向委辦機關確認分級並**請將契約中的資訊安全條款，以附件上傳至請購單**。

選「否」者請在以下 4 個構面分別評估，取最高的做為分級結果。

系統若發生資安事故【機密性(未經授權揭露/外洩)、完整性(資訊錯誤/遭竄改)、可用性(存取/使用中斷)受影響時】的影響程度	
構面 1：營運	■不會造成本院業務停止營運或可於極短時間內恢復營運 (普) □會造成本院部分業務停止營運 (中) □會造成本院全部業務停止營運 (高)
構面 2：資產	■最大會造成本院 20%的資產損失/賠償 (普) □最大會造成本院 50%的資產損失/賠償 (中) □最大會造成本院超過 50%的資產損失/賠償 (高)
構面 3：信譽	■需由一級主管出面處理 (普) □需由單位主管出面處理 (中) □需由院長室主管出面處理 (高)
構面 4：法遵	□無(普) ■行政罰則(如個資法)(中) □刑事責任(高)

二、依據 111 年 06 月 01 日經濟部技術處經科技字第 11103386750 號函行政院訂定「資通系統籌獲各階段資安強化措施」，**務必在編列資通系統之資訊經費時，將資安項目納入考量，並至少編列資訊經費之 5%(含)以上為資安經費**，並依實際情況，執行項目成本分析如下表：

項次	資安項目	資訊經費之百分比
1	系統開發	-
1-1	安全軟體發展生命週期(SSDLC)設計及檢核作業	%
1-2	系統資安防護基準符規作業	%
2	系統及設備維運	-
2-1	系統資安檢測及弱點修補	5 %
2-2	系統備份還原及持續營運演練	%
3	資通安全教育訓練	%
4	其他： (請自行列舉)	%
資安經費占資訊經費合計(不須每項都編列，但合計至少 5%)		5 % **(請填合計)**

三、請購部門已指派**請購人【工號：**537643 **姓名：**魏靖哲**】擔任本購案資安負責人，並瞭解以下資安事項**，請將各項目閱讀後勾選「我已瞭解」始可辦理資通系統委外。

我已瞭解	資安負責人應辦理訂定、監督及確認事項
☑	1. **資安負責人應**監督、確認開發團隊於系統開發時遵循安全軟體開發生命周期(SSDLC)。
☑	2. **資安負責人應於**專案重點里程碑中檢視履約(執行)程序與成果之相關資安管理作為。
☑	3. **資安負責人應**訂定服務等級協議(SLA)，載明服務水準及品質需求，例如：正常運作時間百分比、運作資源消耗、修復時間、系統反應時間、錯誤率、系統與通訊保護完整性等資通系統防護控制措施、跨平台/跨瀏覽器支援程度、使用者感受等。
☑	4. **資安負責人應**確認廠商落實「廠商資安聲明書」的資安要求。
☑	5. **資安負責人應**確認廠商在資通系統上線前已完成安全性檢測(應符合廠商資安聲明書第十五項要求)，並填寫「資通系統上線檢核表」。
☑	6. **資安負責人應**確認資通系統已完成資安法要求之資通系統防護基準，並更新於「附件一、資通系統防護基準查檢表」，以備主管機關查核。
☑	7. 依據《本院對外網站暨數位平台應用管理辦法》，資訊處將於年度間進行年度查核作業，**資安負責人應配合**提供審查所需資料。
☑	8. 依據《本院資訊作業委外安全管理準則》，資訊處將於年度間進行資通委外稽核，**資安負責人應配合**協調廠商，共同辦理資安實地稽核作業。
☑	9. 如本購案是因執行計畫需求，**資安負責人應**將相關之契約(如政府委辦/補助契約)資安要求檢附於本購案請購單以利廠商遵循。
☑	10. 如本購案執行過程發生資安事件，**資安負責人應**立即通報本院資安事件通報窗口 18899。
☑	11. **資安負責人應**配合資安法推動小組辦理之資通安全教育訓練，並於期限內完成訓練。(自 112 年 4 月 1 日起請購單系統將自動檢核請購人已完成資通安全專業課程才可進行填單，請參考資安法推動專區網站查詢最新課程資訊 https://csma.itri.org.tw/)

※ 請購階段由請購人(資安負責人)完成此表，即可存檔上傳至請購單不需要列印出來，將由請購單系統執行簽核流程，並由採購人員提供廠商簽署「廠商資安聲明書」

※ 購案開立後尚未結案前如有更換資安負責人，請告知新資安負責人相關注意事項並交接文件

※ 本表單填寫如有任何問題，請聯繫資通安全管理法推動小組 cybersecurity@itri.org.tw 或資訊處服務窗口 18899，謝謝。

工業技術研究院
Industrial Technology Research Institute

廠 商 資 安 聲 明 書

廠商填寫
本表單適用
資通系統

本廠商參加財團法人工業技術研究院招標採購[　LSMS 系統優化、滿意度問卷電子化　](以下簡稱本案)之投標，茲聲明如下：

項次	聲明事項	是	否
一	本廠商遵守資通安全管理法、其相關子法及主管機關所頒訂之各項資通安全規範及標準，並遵守貴院資通安全管理及保密相關規定。		
二	本廠商執行本案之相關程序及環境，具備完善之資通安全管理措施(如依據數位發展部資通安全署提供之範本建立並落實資通安全維護計畫)或通過第三方驗證。		
三	本廠商參與本案之成員中，至少具備一張資通安全專業證照(依據數位發展部資通安全署最新公告要求)，或具有類似業務經驗之資通安全專業。		
四	本廠商經貴院同意將本案複委託予第三人時，本廠商將要求並監督第三人符合貴院要求之資通安全維護措施。		
五	本廠商同意若因執行本案涉及國家機密時，執行本案之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。		
六	本廠商如涉及利用非自行開發之系統或資源者，將確保其來源合法性，並應標示非自行開發之內容與其來源及依貴院要求提供授權證明。		
七	本廠商訂有資安事件通報與處理流程，如有違反資通安全相關法令或知悉發生資通安全事件時，將立即(1 小時內)通知貴院承辦人及資安事件通報窗口(03-591-8899)，提出緊急應變處置，並配合貴院做後續處理。		
八	本廠商於本案終止或解除時，將返還、移交、刪除或銷毀履行本案而持有之資料(包括但不限於開發需求規格書、原始碼或程式等)，並留存相關紀錄或切結書(附件二)供貴院確認。		
九	本廠商同意貴院得定期或於發生可能影響本案之資通安全事件時，以派員稽核或其他適當方式確認本案之執行情形，並依貴院要求期限內完成改善作業，未依限完成者，依本聲明書計收懲罰性違約金。		
十	本廠商同意本案所提供或使用之資通訊產品(含軟硬體及服務)不得為大陸廠牌，執行本案之團隊成員(含分包廠商)亦不得有陸籍人士參與。		
十一	本廠商同意本案所提供的產品或服務之所屬一切資料存取、備份及備援之實體所在地，不得有置於中國大陸地區(含香港、澳門)或跨該等境內傳輸相關資料之情形。		
十二	本案若有提供資通服務(例如主機/網站空間租用等)，本廠商所提供之資通服務，**如涉及貴院對外網站/系統/服務，應具備已通過 ISO 27001 驗證**或具有同等或以上效果之系統或標準驗證，並確保其證書有效性。		
十三	本廠商將確保本案符合以下資訊安全要求，並依貴院要求交付相關文件： 1. 測試區應進行權限控管，並確保測試環境安全。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。 2. 開發/測試及上線環境應安裝防毒軟體及更新病毒碼，並執行作業系統安全性更新。 3. 確實執行組態管理(原始碼管理、版本控制及系統發展生命週期之相關文件...等)，以確保系統之完整性及一致性，並依資安管理相關規範提供權限控管與存取紀錄保存。 4. 本案將針對受委託範圍自行辦理資安稽核作業，並留存稽核紀錄供貴院備查。 5. 遵守貴院其他資訊安全要求，例如：進入貴院實體環境或存取貴院網路/資訊系統應事先提		

	出申請並取得核准、因執行本案需求依貴院要求申請之工研院帳號使用時遵守「工研院電腦與網路使用行為準則」、知悉或持有工研院機密資訊時遵守「工研院機密資訊管理辦法」...等。		
十四	本廠商之「承接的資通系統開發/維運之相關程序及環境」應通過資訊安全管理第三方驗證，且於專案執行期間持續有效，並提供廠商資安第三方驗證資料表(附件三)。 本廠商如未具備前述條件，已知悉驗收交付時除現有須完成弱點掃描之規定外，須以商用軟體執行程式碼源碼掃描或滲透測試(範圍涵蓋本案提供之資通系統前/後台及資通服務)，並修補至無高風險，購案執行過程須配合貴院資安小組實地稽核並限期改善。		
十五	本廠商及執行本案之成員應以善良管理人之注意，妥善保管因執行本案而知悉或持有之相關資料，並採取適當之保密措施，非經貴院事前書面同意，不得逆向解析(reverse engineer、reverse assemble 或 de-compile)、洩漏或交付予任何第三人。執行本案之成員違反前開規定致生之一切損害，本廠商負連帶賠償責任。		
十六	本廠商依據本案之資通系統防護需求分級(☐普 ☐中 ☐高)，確認交付之資通系統已符合資安法「資通系統防護基準」所訂之控制措施，並提供資通系統防護基準查檢表(附件一)。		
十七	本廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，提出安全性檢測證明(檢測範圍涵蓋本案提供之資通系統前/後台及資通服務)，並出具至少已修正至無高風險以上等級弱點之掃描報告。(註：如採購規範書或委辦契約有其他修正風險等級弱點之規定者，從嚴規定。) 安全性檢測掃描工具為取得授權使用的商用軟體，於每次弱點掃描前，將工具之弱點資料庫更新至最新版本，並提供佐證資料，以確保完整正確。 若契約價金達新台幣 1,000 萬(含)以上，本廠商應提供由公正第三方出具之檢測報告。 本廠商同意於本案驗收後一年內，配合貴院定期安全性檢測作業，如有發現高風險以上等級弱點，依貴院通知時限內進行修補作業。		
附註	**任一項目答「否」或未答者，不得參加投標；其投標者，不得作為決標對象；內容有誤或自行修改者，不得作為決標對象。**		

本廠商以上聲明全屬真實，如有聲明不實，本廠商應按契約價金總額 20 %，計收懲罰性違約金，本廠商亦同意貴院保有終止或解除契約之權；如因聲明不實或違反政府法令致貴院受有損害，本廠商願負相關法律及損害賠償責任。

本廠商已收到下列文件，並已於報價前釐清所有疑問。

☑廠商資安聲明書 ☑資通系統上線檢核表 ☑附件一、資通系統防護基準查檢表

☑附件二、資料返還、刪除、銷毀切結書 ☑附件三、廠商資安第三方驗證資料表

投標廠商填表人：

本案廠商資安負責人： 連絡電話：

投標廠商名稱：

投標廠商公司章及廠商負責人章： 日期：

【重要提醒】本案執行期間如《資通安全管理法》及其相關子法規定經主管機關修正者，應依最新法令規定辦理。

工業技術研究院
Industrial Technology Research Institute

資通系統上線檢核表

請購部門
上線測試或驗收時
填寫

為協助全院各單位辦理資通委外案件落實資通安全管理法(及子法)與主管機關之要求(如資通系統籌獲各階段資安強化措施)，訂定本表，請購部門上線測試或驗收時完成填寫，經核決主管同意後自行留存，以備資安法推動小組及主管機關查核之需要。

項次	檢核項目	檢核結果	
一	資通系統防護基準查檢表	☐廠商已提交「附件一、資通系統防護基準查檢表」，並經檢核完成本案防護需求 ☐普 ☐中 ☐高 級所有控制措施 ☐部分控制措施尚未完成(由單位資推委員核決) 原因：	
二	資通系統安全性檢測報告	☐廠商已提交 1.無高風險之資通系統(需涵蓋前/後台)安全性檢測報告、2.無高風險之資通服務(如主機)安全性檢測報告、3.安全性檢測工具授權證明及確認弱點資料庫更新至最新版本 ☐前列三項中第☐1☐2☐3 項無法提交(由單位資推委員核決) 原因：	
三	資通系統安全管理第三方驗證	☐廠商「承接的資通系統開發/維運之相關程序及環境」已通過資通安全管理第三方驗證，並提交「附件三、廠商資安第三方驗證資料表」 ☐廠商「承接的資通系統開發/維運之相關程序及環境」尚未通過資通安全管理第三方驗證，但已提交以商用軟體執行程式碼源碼掃描或滲透測試(範圍涵蓋本案提供之資通系統前/後台及資通服務)，並修補至無高風險 ☐前述兩項廠商皆未符合(由單位資推委員核決) 原因：	
四	廠商已返還、移交、刪除或銷毀履行本案而持有之資料（包括但不限於開發需求規格書、原始碼或程式等）	☐廠商已提交 ☐切結書(附件二) 或 ☐處理紀錄 ☐廠商未提交切結書或處理紀錄(由單位資推委員核決) 原因：	
五	資通系統基本資料	☐本案僅交付程式碼(以下第五項、第六項及第七項免填寫)	
		是否因承接政府計畫建置	☐是 ☐否
		是否包含個資	☐是 ☐否
		是否有管理後台	☐是 ☐否
		是否屬於本院對外網站	☐是，且已完成登錄 ☐是，尚未完成登錄(由單位資推委員核決) ☐否
		上線網址	https://
六	上線後維運管理 (如尚未完成上線作業， 請說明原因： 由單位資推委員核決)	主機所在機房： ☐工研院資訊處 itriCloud ☐工研院資訊處 webhosting ☐其他通過 ISO 27001 驗證之機房 _____	

		主機(Web Server)維運管理： ☐本院管理：　(工號+姓名) ☐廠商管理：　(廠商名稱+姓名+連絡電話) ☐其他：　(說明狀況)
		資料庫(DB Server)維運管理： ☐本院管理：　(工號+姓名) ☐廠商管理：　(廠商名稱+姓名+連絡電話) ☐其他：　(說明狀況)
		資通系統(Application)維運管理： ☐本院管理：　(工號+姓名) ☐廠商管理：　(廠商名稱+姓名+連絡電話) ☐其他：　(說明狀況)
七	資通系統重要檢查項目 (任一項目無法完成者，由單位資推委員核決，並說明原因：　)	☐已採用 HTTPS 加密傳輸 ☐主機、資料庫、資通系統均已完成備份 ☐主機已安裝防毒軟體並設置網路防火牆 ☐帳號皆已具備密碼複雜度要求並定期修改，或不具備一般使用者/管理者帳號機制 ☐針對重要日誌及管理者操作日誌，已留存 6 個月以上 LOG ☐使用預設密碼之元件或軟體已完成密碼修改 ☐已移除或停用廠商操作之帳號或確認符合實際最小權限設定原則 ☐已確認廠商交付軟體元件清單(SBOM)，內容包含元件版本及授權資訊，並完成第三方元件安全性檢視及提供佐證資料。[註] 註：廠商已提供無高風險漏洞之第三方元件安全性檢測報告，或人工檢視確認無 CVSS 分數≧7.0 之已知安全漏洞佐證。如有無法修補之高風險漏洞應說明原因及已採行或規劃之有效改善作法(例如：已建置其他有效防護機制、已另案規劃升級或汰換處理等)，並經資推委員核決。

請購部門已確認完成檢核表之所有項目，由請購部門主管或計畫主持人核決。

如有任一項目無法完成，由單位資推委員核決，並送至資通安全管理法推動小組列管。請於單位資推委員核決後將表單掃描 Email 至 cybersecurity@itri.org.tw 並說明無法完成原因。

資安負責人：	核決人：	
(請購單之請購人)	(請購部門主管或計畫主持人)	(單位資推委員)
工號：	☐同意驗收	☐同意驗收
姓名：	☐不同意驗收	☐不同意驗收
職稱：		
日期：　年　月　日	日期：	日期：

附件一

資通系統防護基準查檢表

說明：

1. 廠商填寫完後由請購部門留存。
2. 未於本購案範圍或尚未達成之控制措施，應由本院請購部門依資安法要求完成。
3. 請本院請購部門或系統負責人適時更新此份資訊，以備主管機關查核。

一、資通系統基本資料

系統名稱	工研院產業學習網報名系統
系統網址	https://reglsms.itri.org.tw/666C9E4B-206F-4AC1-9A17-777A4F506BB7/IMUFOQqkt7hJxRl%ef%bc%8f2bHEGPrS5FFUfqelRf9RUvNjOII%ef%bc%9d
主機所在位置 依據經濟部技術處 110 年 12 月 29 日經科技字第 11003409910 號函要求，資通系統/網站部署之機房運作應通過 ISO 27001 驗證。	☐工研院資訊處 itriCloud ■工研院資訊處 webhosting ☐其他通過 ISO 27001 驗證之機房_____ 註：煩請檢附該機房通過 ISO 27001 驗證之證書。
主機作業系統及版本	■Windows，版本: WINSVR2022_ ☐Mac OS，版本:_____ ☐Unix / Linux，版本: _____ ☐FreeBSD，版本: _____ ☐其他，作業系統名稱_____，版本:_____ 註：煩請寫出「種類」和「版本號碼」，如 Linux 請寫 CentOS 6.8、RHEL 6.8、Oracle Linux 6.8 或其他，而非只寫 Linux 6.8，以利查出明確漏洞資訊。
開發語言及版本	☐C/C++，版本:_____ ■C#，版本:_ 10_____ ☐Java，版本:_____ ☐JavaScript，版本:_____ ☐Python，版本:_____ ☐PHP，版本:_____ ☐Visual Basic .NET，版本: _____ ☐其他，語言名稱_____，版本:_____ 註：煩請填寫詳細版本，如 PHP 請寫 7.3.17 或其他，而非 PHP 7.0。
Web 伺服器	☐無 ☐有， ☐Apache HTTP Server，版本:_____ ☐Apache Tomcat Server，版本:_____ ■Microsoft IIS，版本：10___ ☐Nginx，版本:_____ ☐其他，伺服器名稱_____，版本:_____ 註：煩請填寫詳細版本，如 Tomcat 請寫 7.0.65 或其他，而非 Tomcat 7.0。

<table>
<tr><td>資料庫</td><td>☐無
☐有，
☐ DB2，版本:_____
☐ Sqlite，版本:_____
☐ Oracle，版本:_____
☐ MySQL，版本:_____
☐ PostgreSQL，版本:_____
☐ Microsoft Access，版本:_____
■ Microsoft SQL Server，版本: (資訊處管理)
☐其他，資料庫名稱_____，版本:_____
註：煩請填寫詳細版本，如 Oracle Database 請寫 12.1.0.1，而非僅寫 12。</td></tr>
<tr><td>網站框架</td><td>☐無
☐有，
☐ Struts，版本:_____
☐ Spring，版本:_____
☐ ZK，版本:_____
☐ django，版本:_____
☐.Net Framework，版本: _____
■其他，網站框架名稱_.NET Core__，版本:_____
註：煩請填寫詳細版本。</td></tr>
<tr><td>第三方服務</td><td>雲端平台 ■無 ☐有，_____
外部 API ■無 ☐有，_____
☐其他 _____</td></tr>
<tr><td>軟體元件清單</td><td>☐使用第三方軟體元件如下，已完成安全性檢視，並檢附相關佐證資料。如採用安全性檢測工具，請檢附無高風險漏洞之第三方元件安全性檢測報告(如 Sonatype 掃描報告)；如以人工方式檢視，請檢附確認無 CVSS 高風險等級以上(CVSS 分數≧ 7.0)之已知安全漏洞相關佐證資料。
高風險之漏洞原則應完成修補，如無法完成修補，應敘明原因並採取其他有效改善或補償措施，且經請購單位評估風險可接受性後同意。
(如無法修補高風險漏洞，請敘明原因及其他有效補償措施)
<table>
<tr><td>元件名稱(以下可自行新增表格)</td><td>版本(請填詳細版本)</td><td>授權資訊</td></tr>
<tr><td>(範例) log4j</td><td>(範例) 2.24.3</td><td>(範例) Apache License 2.0</td></tr>
<tr><td>(範例) Bootstrap</td><td>(範例) 5.3.8</td><td>(範例) MIT License</td></tr>
<tr><td>(範例) jQuery</td><td>(範例) 3.7.1</td><td>(範例) MIT License</td></tr>
<tr><td>(範例) Ckeditor</td><td>(範例) 4.25.1-lts</td><td>(範例) Commercial License</td></tr>
<tr><td>(範例) ClosedXML</td><td>(範例) 0.104.2</td><td>(範例) MIT License</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>首次上線日期</td><td>2026 年 5 月 18 日</td></tr>
<tr><td>最近改版日期</td><td>年 月 日</td></tr>
</table>

資通系統防護需求分級	☐普 ☐中 ☐高

二、資通系統防護基準查檢表(依據 115/01/07 修正之資通安全責任等級分級辦法)

若對以下內容需要進一步瞭解，請至國家資通安全研究院(NICS)>資安資源>參考文件>共通規範>下載「資通系統防護基準驗證實務」。

網址：https://www.nics.nat.gov.tw/cybersecurity_resources/reference_guide/Common_Standards/

※ 原則上應符合系統對應等級之全部控制措施（普級：符合普級；中級：符合普級與中級）。若委託範圍未涵蓋該控制措施，請勾選「不適用」。

等級	構面	措施	控制措施	檢查結果
普級	存取控制	帳號管理	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	☐是，請勾選已具備之程序： ☐帳號申請 ☐帳號建立 ☐帳號修改 ☐帳號啟用 ☐帳號停用 ☐帳號刪除 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	存取控制	帳號管理	已逾期之臨時或緊急帳號應刪除或禁用	☐是，請勾選實作方式： ☐人工審查 ☐系統自動刪除或禁用 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	帳號管理	資通系統閒置帳號應禁用。	☐是，請勾選實作方式： ☐人工審查 ☐系統自動刪除或禁用 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	帳號管理	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	☐是，定期審查週期_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	存取控制	最小權限	採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	遠端存取	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	☐是，已有遠端存取的文件化資訊。 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	遠端存取	使用者之權限檢查作業應於伺服器端完成。	☐是，請勾選實作方式： ☐於伺服器端進行權限檢查 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	遠端存取	應監控遠端存取機關內部網段或資通系統後臺之連線。	☐是，已有監控機制 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	存取控制	遠端存取	應採用加密機制。	☐是，請勾選實作方式： ☐ HTTPS 加密 ☐ SSH 加密 ☐ VPN 加密 ☐遠端桌面通訊協定(RDP)啟用加密 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	遠端存取	遠端存取之來源應為機關已預先定義及管理之存取控制點。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	記錄事件	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	☐是，已保留 6 個月事件日誌 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	事件日誌與可歸責性	記錄事件	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	☐是，請勾選實作方式： ☐記錄身分驗證事件 ☐記錄資料存取事件 ☐記錄系統功能錯誤事件 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	記錄事件	應記錄資通系統管理者帳號所執行之各項功能。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	☐是，請勾選實作方式： ☐事件類型 ☐發生時間 ☐發生位置 ☐使用者身分識別 ☐採用單一的日誌機制 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	事件日誌與可歸責性	日誌儲存容量	依據日誌儲存需求，配置日誌紀錄所需之儲存容量。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	日誌處理失效之回應	資通系統於日誌處理失效時，應採取適當之行動。	☐是，請勾選實作方式： ☐關閉資訊系統 ☐覆寫最舊的日誌紀錄 ☐停止產生日誌紀錄 ☐通知管理者進行故障排除 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	時戳及校時	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間 (UTC)或格林威治標準時間(GMT)。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	事件日誌與可歸責性	時戳及校時	系統內部時鐘應定期與基準時間源進行同步。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	日誌資訊之保護	對日誌之存取管理，僅限於有權限之使用者。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	營運持續計畫	資料備份	訂定資料可容忍損失之時間要求。	☐是，資料可容忍損失之時間(RPO 值)為_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	營運持續計畫	資料備份	執行資料備份。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	營運持續計畫	系統備援	訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。	☐是，最大可容忍中斷時間為_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	使用者之識別與鑑別	資通系統應識別及鑑別使用者，並禁止使用者共用帳號。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	識別與鑑別	身分驗證管理	使用預設密碼初次登入系統時，應於登入後立即變更。	☐是，要求初次登入立即變更預設密碼 ☐不適用： ☐未使用預設密碼 ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	身分驗證管理	身分驗證相關資訊不以明文傳輸。	☐是，請勾選實作方式： ☐使用 HTTPS 或 SSH 加密 ☐將身分驗證資訊加密或編碼後傳輸 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	身分驗證管理	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	☐是，具備帳戶鎖定機制 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	識別與鑑別	身分驗證管理	使用密碼進行驗證時，應強制最低密碼複雜度；依機關密碼效期規定變更密碼。	☐是，請勾選實作方式： ☐密碼最小長度_____ ☐密碼須包含下列字元類型，至少符合_____種： ☐英文大寫 ☐英文小寫 ☐數字 ☐特殊符號 ☐機關密碼最短效期_____ ☐機關密碼最長效期_____ ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	身分驗證管理	密碼變更時，至少不可以與前 3 次使用過之密碼相同。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	識別與鑑別	身分驗證管理	系統密碼複雜度、效期及變更控制措施，對外部使用者，得由機關自行規範辦理。	☐是，對外部使用者規範與實作方式： ☐密碼最小長度_____ ☐密碼須包含下列字元類型，至少符合_____種： ☐英文大寫 ☐英文小寫 ☐數字 ☐特殊符號 ☐機關密碼最短效期_____ ☐機關密碼最長效期_____ ☐密碼變更不可與前___次相同 ☐其他 _____ ☐不適用： ☐系統無外部使用者 ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	鑑別資訊保護	資通系統應遮蔽鑑別過程中之資訊。	☐是，請勾選實作方式： ☐輸入密碼時顯示*或空白 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)進行確認。	☐是，以本表單進行確認 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期開發階段	應針對安全需求實作必要控制措施。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	系統與服務獲得	系統發展生命週期開發階段	應注意避免軟體常見漏洞及實作必要控制措施。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期開發階段	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期測試階段	執行「弱點掃描」安全檢測。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
普級	系統與服務獲得	系統發展生命週期部署與維運階段	於部署環境中應針對相關資通安全威脅，進行更新與修補。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期部署與維運階段	識別並關閉不必要服務及埠口。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期部署與維運階段	資通系統不使用預設密碼。	☐是，本系統、資料庫或 Web 伺服器等軟體元件未使用預設密碼 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期部署與維運階段	執行系統源碼備份。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	☐是，已將資安要求納入委外契約 ☐不適用： ☐無委外 ☐其他，請說明：_____
	系統與服務獲得	獲得程序	識別資通系統使用之第三方軟體、服務、函式庫或其他元件。	☐是，已交付軟體元件清單(SBOM)，並包含元件版本及授權資訊 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統文件	應儲存與管理系統發展生命週期之相關文件。	☐是 ☐不適用，請說明：_____

等級	構面	措施	控制措施	檢查結果
	系統與資訊完整性	漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	☐是，已定期進行軟體元件漏洞修復與更新 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與資訊完整性	資通系統監控	發現資通系統有被入侵跡象時，應通報機關特定人員。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與資訊完整性	軟體及資訊完整性	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
資通系統防護需求分級為[普]者，填寫到此結束 資通系統防護需求分級為 [中]或[高]者，請繼續往下填寫				
中級	存取控制	帳號管理	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。	☐是，請勾選實作方式： ☐機關定義閒置時間_____ ☐其他_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	存取控制	帳號管理	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。	☐是，系統自動將使用者登出 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	記錄事件	應定期審查機關所保留資通系統產生之日誌。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	事件日誌與可歸責性	日誌資訊之保護	應運用雜湊或其他適當方式之完整性確保機制。	☐是，請勾選實作方式： ☐提供日誌資訊之雜湊值 ☐使用異地備份進行完整性驗證 ☐使用目錄監控軟體偵測檔案異動 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	營運持續計畫	資料備份	應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。	☐是，定期測試週期_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	營運持續計畫	系統備援	應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。	☐是，定期測試週期_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	身分驗證管理	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	☐是，請勾選實作方式： ☐CAPTCHA ☐帳戶鎖定機制 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
中級	識別與鑑別	身分驗證管理	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	☐是，請勾選實作方式： ☐寄發 EMAIL 驗證連結 ☐寄發簡訊驗證碼 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	識別與鑑別	鑑別資訊保護	資通系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。	☐是，請勾選實作方式： ☐密碼加密儲存 ☐密碼雜湊儲存 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期設計階段	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期設計階段	將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與服務獲得	系統發展生命週期部屬與維運階段	於系統發展生命週期之維運階段，應執行版本控制與變更管理。	☐是，版本控制工具/方式_____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

等級	構面	措施	控制措施	檢查結果
	系統與服務獲得	獲得程序	開發、測試及正式作業環境應為區隔。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與資訊完整性	漏洞修復	定期確認資通系統相關漏洞修復之狀態。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與資訊完整性	資通系統監控	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
中級	系統與資訊完整性	軟體及資訊完整性	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	☐是，請勾選實作方式： ☐目錄監控(如 Linux inotify 等工具) ☐使用雜湊機制 ☐其他 _____ ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____
	系統與資訊完整性	軟體及資訊完整性	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	☐是 ☐不適用： ☐委託範圍未包含此控制措施 ☐其他，請說明：_____

附件二

資料返還、刪除、銷毀切結書

本廠商保證已返還、刪除或銷毀履行本案(案件名稱:＿＿＿＿＿＿＿＿＿＿)而持有之所有資料及其影本、複製本(包括但不限於開發需求規格書、原始碼或程式等),且確實監督並確認參與本案之相關人員未以任何形式留存、洩漏或交付予第三人,亦不得為自己或第三人利益而使用。若有洩漏、交付、使用、竄改或其他不利貴院之相關行為，本廠商同意依照本案契約價金總額 20％,支付懲罰性違約金予貴院,並賠償貴院因此所受之一切損害，且應自行承擔相關民、刑事責任，絕無異議。

此致

財團法人工業技術研究院

廠商填表人簽名：

廠商名稱：

廠商公司章及負責人章：

日期：

附件三

廠商資安第三方驗證資料表

自 2025 年 4 月起工研院資通系統委外廠商之「承接的資通系統開發/維運之相關程序及環境」皆應通過資訊安全管理第三方驗證，請廠商於驗收上線前提供通過第三方驗證相關資訊，並附上第三方驗證證書掃描檔，以利請購人及資安小組確認。(若第三方驗證資料有更新，請再次填寫本表)。

公司名稱	按一下或點選這裡以輸入文字。	
公司地址	按一下或點選這裡以輸入文字。	
公司統編	按一下或點選這裡以輸入文字。	
聯絡資訊	姓名：按一下或點選這裡以輸入文字。 電話：按一下或點選這裡以輸入文字。 Email：按一下或點選這裡以輸入文字。	
	是否同意上述聯絡資訊供本院同仁業務洽詢使用？(未勾選表示不同意)	☐同意，請填妥後寄至 cybersecurity@itri.org.tw ☐不同意
第三方驗證資訊	驗證項目及版本：(例如 ISO 27001:2022、CNS 27001:2023) 驗證機構：(例如 SGS、BSI) 證書編號：(請依照證書上的資訊填寫) 驗證有效期間：有效期間-起至有效期間-止 驗證範圍： (請依照證書上的資訊填寫，中英文皆可)	
	請確認以下檢核項目	
	☐已確認驗證範圍包含「承接的資通系統開發/維運之相關程序及環境」，並標示於證書掃描檔或上方文字方塊中 ☐已確認證書上的公司名稱、地址與公司營業登記資料相符 ☐將證書掃描檔與本資料表一併繳交	

廠商公司章及負責人章：

日期：