

國立雲林科技大學

資訊採購委外廠商資通安全規範切結書

本校資訊採購單位：_____

填表日期： 年 月 日

資訊採購項目：_____

本文件說明國立雲林科技大學(以下簡稱本校)規範委外廠商(以下簡稱受託者)提供**資通訊產品**¹時必須遵守事項。簽署時，表示受託者已閱讀、瞭解並同意接受本文件之所有內容。

本校資訊安全規範事項如下：

一、所有資通訊產品、資訊服務採購適用：

1. 受託者遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本校資通安全管理(ISMS)及保密相關規定。
2. 受託者提供之資通訊產品，原則不得為「危害國家資通安全之產品(大陸廠牌資通訊產品)」。
3. 受託者於本採購承接範圍內，因未採取適當防護，致本校敏感/個人資料外洩或遭竄改時，願負相關法律責任。

二、☐資訊服務²採購另適用以下事項：

1. 受託者團隊成員於執行業務前，應完成簽署【委外廠商保密切結書】並提交本校。
2. 契約履約或終止後，受託者應依本校之指示，刪除或銷毀執行服務所持有之相關機敏資料，或依本校之指示返還或移交之，並填寫【系統資料返還移交銷毀刪除切結書】提交本校。
3. 受託者應具備完善之【資通安全管理措施】³或通過第三方驗證；並設置 1 名資通安全專業人員(專責管理本案)，負責推動、協調及督導本案委外作業，確認履約階段作業符合本校及受託者雙方之資安管理規範；受託者團隊成員需擁有今年度 3 小時以上之【資通安全專業課程訓練證明】或【資通安全專業證照】或【具有類似業務經驗】；受託者負責本案之人員變動時，應通知本校承辦人員。
4. 受託者團隊成員不得為陸籍人士，且不得提供及使用危害國家資通安全之產品(大陸廠牌資通訊產品)，使用資訊設備時應遵守本校相關安全管控措施(例如帳密管理、遠端連線、機房進出等)。
5. 受託者知悉發生資安事件應於 1 小時內通知本校(或接獲本校通知 1 小時內)，並採取適當之應變措施；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。

¹「資通訊產品」定義：參考資通安全管理法第 3 條用詞定義，包含軟體、硬體及服務等項，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品。

² 資訊服務：指提供與電腦軟體或硬體有關之服務；包括整體規劃、系統整合、系統稽核、系統管理、網路管理、軟體開發、軟體驗證、軟體維護、硬體維護、硬體操作、機房設施管理、備援服務、網路服務、顧問諮詢、資料庫建置、資料處理、資料登錄或訓練推廣等服務。

³ 得採取填寫本校 ISMS-D-055-委外廠商資訊安全要求查核表作為佐證。

6. 本校依<<資通安全管理法施行細則>>保有定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形之權利，稽核結果不符合各項資通安全規範者，於接獲本校通知後應於期限內完成改善。
7. 若本案所約定之部分服務有分(轉)包情形，受託者應以書面方式或電子郵件告知本校並獲得同意，且受託者應與分(轉)包廠商書面約定，分(轉)包廠商亦應符合本案資通安全規定要求，惟受託者對於分(轉)包廠商履約之部分，仍應負完全責任。
8. 通訊與雲端服務之限制：受託者及其所供應之財物(軟硬體設備)或勞務之資料存取、儲存、備份及備援等作業，其實體或雲端所在地及資料傳輸不得跨境至大陸地區(含香港及澳門地區)。受託者於本案建置或使用雲端服務時，請參考國家資通安全研究院之共通規範專區所公布「政府機關雲端服務應用資安參考指引」。
9. 本採購案若涉及國家機密者，受託者團隊成員應接受本校適任性查核，並依國家機密保護法之規定，管制其出境。

三、☐資通系統相關⁴另適用以下事項：

1. 本案資通系統防護需求等級為 級，受託者應依資通安全責任等級分級辦法附表十所定資通系統防護基準執行控制措施，並繳交【資通系統防護基準查核表】。
2. 受託者交付之軟硬體及文件，應確保無內藏惡意程式及隱密通道，且應在上線前進行主機及網站弱點掃描並繳交【弱點掃描報告】；針對非自行開發之系統或資源(例如框架、套件、外掛程式)，應標示內容與其來源及提供授權證明。
3. 須配合本校及上級機關資安政策(例如:攻防演練、入侵偵測、弱點掃描等資安措施)，若發現待改善風險或漏洞，受託者應協助修補系統問題。
4. 本校認定之資通系統應配合本校指定流程進行業務持續運作演練，確保系統緊急中斷、災害發生時之應對處理，受託者應配合辦理。
5. 當系統發生重大事故、中斷、錯誤無法運行，或系統無法復原之情境，受託者應協助將備援資料還原至設備並再度啟用系統，令該業務得持續進行

受託者公司（單位）名稱：

負責人簽章：

公司大小章：

⁴ 資通系統相關係指系統建置、系統整合、系統稽核、系統管理、軟體開發、軟體驗證、軟體維護等