1. 國立中央大學附屬中壢高級中學

委外廠商執行人員保密切結書

立切結書人 洪志遠 (簽署人姓名)等，受 說說而已科技有限公司 (廠商名稱)委派，處理國立中央大學附屬中壢高級中學（以下稱本校） 自主學習行政管理系統 (資通業務名稱)，謹聲明恪遵本校下列工作規定，並對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經本校權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 應主動了解本校資安責任等級，並依該項業務之防護等級進行各項工作。

二、 應主動了解並遵守本校相關法令及規範，如「資通安全政策」等。

三、 未經申請核准，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

四、 未經本校業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本校網路。若經申請獲准連接本校網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

五、 經核准攜入之資訊設備欲連接本校網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

六、 廠商駐點服務及專責維護人員原則應使用本校配發之個人電腦與週邊設備，並僅開放使用本校內部網路。若因業務需要使用本校電子郵件、目錄服務，應經本校業務相關人員之確認並代為申請核准，另欲連接網際網路，亦應經本校業務相關人員之確認，並代為申請核准。

七、 本校得定期或不定期派員稽核立切結書人是否符合上列工作規定。

八、 本保密切結書不因立切結書人離職而失效。

九、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人姓名及簽章：洪志遠

立切結書人所屬廠商：說說而已科技有限公司

廠商名稱及蓋章 說說而已科技有限公司

廠商負責人姓名及簽章 洪志遠

廠商負責人聯絡電話及地址 04-22385456 臺中市北區崇德路一段631號17樓之2

中 華 民 國 114 年 7 月 11 日

國立中大壢中委外廠商查核暨自我檢核項目表

查核人員：許元彰　　填表日期：　114 年 7 月 4 日

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全責任	1.1 是否知悉甲方資安等級？	□	■	□	甲方尚未正式提供資安責任等級聲明，建議提供書面確認或引用法規分級。
	1.2 是否是否知悉合約標的之系統防護基準？	□	■	□	雖甲方未提供防護基準文件，本系統已內建基本防護機制（權限分級、SSL/TLS、日誌），建議甲方補充正式防護基準文件以資佐證。
	1.3 是否了解甲方資安維護計畫對合約標的系統各項要求？	□	■	□	甲方未提供資安維護計畫或書面要求。本公司已主動執行弱掃、日誌保存等基本資安措施，建議甲方提供正式維護計畫以資佐證。
2.應辦事項	2.1 系統是否符合防護基準？	□	■	□	甲方未提供防護基準文件，本公司已執行基本防護措施（權限分級、加密傳輸、日誌管理），建議甲方補充防護基準文件，以明確防護標準。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	2.2 系統是否具備合適備份機制？	□	■	□	已執行每日資料庫備份，但因甲方未提供異地備份機制，目前未達完整備份要求。建議甲方協助提供異地備份資源以強化防護。
	2.3 是否完成系統弱掃，並完成修補中級(含)以上之風險？	□	■	□	本公司已於 2025/07/04 完成弱點掃描，掃描結果中僅剩 CSP 設定待更新以排除中級風險，預計於近期完成修補。
	2.4 是否完成資通安全健診，並完成修補中級(含)以上之風險？	□	■	□	本公司尚未完成資通安全健診，已完成弱點掃描並修補中級以上風險。建議甲方確認是否需委託健診作業或提供相關規範。
	2.5 是否完成滲透測試，並完成修補中級(含)以上之風險？	□	■	□	本公司已以 OWASP ZAP 完成自動化弱點掃描及基礎自動測試，未執行完整滲透測試作業，建議甲方確認滲透測試需求與範圍。
	2.6 是否完成源碼檢測，並完成修補中級(含)以上之風險？	■	□	□	本公司已於 2025/07/04 完成源碼檢測（工具：SonarQube），掃描報告顯示 2 項 high 風險，經人工分析屬誤判，無實際風險。無需修補項目，檢測結果已記錄備查。
	2.7 是否實施之系統日誌管理？	□	■	□	系統具備日誌功能（登入、操作紀錄、異常事件），日誌儲存與管理由甲方主機環境負責。本公司可配合甲方日誌保存與稽核需求。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	2.8 是否配合甲方每年辦理1次業務持續運作演練及1次資通安全事件通報演練？	□	■	□	甲方未安排廠商參與業務持續運作或資安事件通報演練，建議甲方如有辦理時邀請本公司配合參加。
	2.9 是否參加3小時以上資通安全通識教育訓練及3小時以上資通安全專業課程訓練或資通安全職能訓練？	□	■	□	本公司人員尚未參加資安通識及專業訓練，建議安排相關教育課程以符合法規要求。
3.資安風險處理及預防措施	3.1 是否有符合人員及設備安全評估措施？	■	□	□	■人員不得為陸籍 ■設備不得為大陸品牌
	3.2 是否簽署廠商保密同意書、廠商執行人員保密切結書	□	□	□	□廠商保密同意書 □執行人員保密切結書
	3.3 作業環境是否進行合適控管？ □具 ISO27001認證 ■不具 ISO27001認證	□	■	□	□進行資通系統盤點 □進行資通系統風險評估 □有防火牆且有管控規則 ■有日誌管理 ■有合適權限管控

廠商名稱、住址及公司章：說說而已科技有限公司

臺中市北區崇德路一段631號17樓之2

國立中大壢中-委外廠商資安管理作業自評表					
文件編號	CLHS-ISMS-B-007	機密等級	限閱	版本	1.0

填表日期： 114 年 7 月 4 日

委外廠商名稱	說說而已科技有限公司	委外廠商負責人	洪志遠
專案名稱	中大壢中自主學習行政管理系統	單位/專案負責人	洪志遠

評估項目	辦理情形
1.管理面	
1.1辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ ☑辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為____ ☑本專案之資安人員為__黃信賢__ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於____文件，已(將)採取對應之控制措施詳____文件(如未載明於既有文件內，請於備註欄內說明相關措施) ☑未就本專案進行資安風險評估 備註：_____中級_____
1.4本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含____ ☑未就本專案訂定相關資安事件通報及應變程序 備註：_____
1.5由招標公告日起算，過去3年是否發生因管理議題肇因之重大資安事件	☑過去3年無發生因管理議題肇因之資安事件 □是，共__次，事件發生主要根因為____ 備註：_____

國立中大壢中-委外廠商資安管理作業自評表					
文件編號	CLHS-ISMS-B-007	機密等級	限閱	版本	1.0

2.技術面	
2.1本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	☑本專案範圍內之資通系統將規劃執行_____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：__原始碼掃描：前端、後端，弱點掃描：網頁應用程式、Server___ ☐未就本專案範圍內之資通系統規劃安全性檢測 備註：_____
2.2辦理本專案受託業務環境及設備導入之相關資通安全防護措施	☐本專案受託業務之環境及設備已(將)導入(啟用)_____(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：_____ ☑本專案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	☑本專案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：__分級：管理者:使用者資料、報名資料管理、報名者：個人資料維護、查詢__ ☐未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3.認知訓練面	
3.1本專案直接履約相關人員之資安教育訓練	☐本專案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含____；__小時之資安專業教育訓練，對象包含____ ☑未規劃相關資安教育訓練 備註：_____
3.2本專案團隊人員取得之資通安全專業證照	☐本專案具資安證照之團隊成員有：__位 ☑本專案團隊人員未具備資通安全專業證照 備註:_____iPAS資安中級工程師認證中(已通過中級-資訊安全規劃實務科目)_____

廠商用印：