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 8 月 19 日

委外廠商名稱	寶慶文化科技股份有限公司	委外廠商 負責人	王璧慧
專案名稱	M7圖書館自動化系統維護壹年期(114年度)	單位/專案負責人	汪致宇

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_維護合約__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_盧彥碩___ ■本專案之資安人員為_陳宣行___ □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_維護合約___文件，已(將)採取對應之控制措施詳_維護合約___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：_____
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)載明於維護合約__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	■過去3年無發生因管理議題肇因之資安事件

否發生因管理議題肇因之重大資安事件	□是，共__次，事件發生主要根因為____ 備註：_____
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_第三方執行弱點掃描____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：_M7系統____ □未就本專案範圍內之資通系統規劃安全性檢測 備註：_由第3方提弱掃報告，若有需要修正之處，由寶慶公司處理__
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)_防毒軟體、防火牆____(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2__種等級，相關存取控制、權限管理機制說明如下：管理端與使用端___ □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_3_小時之資安通識教育訓練，對象包含_資安人員；__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：_2_位 □本專案團隊人員未具備資通安全專業證照 備註：_____

廠商用印：

國立中大壢中委外廠商查核暨自我檢核項目表

查核人員：汪致宇　　填表日期：　114 年 8 月 19 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？	■	□	□	
	1.2 是否是否知悉合約標的之系統防護基準？	■	□	□	
	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？	■	□	□	
1. 應辦事項	2.1 系統是否符合防護基準？	■	□	□	
	2.2 系統是否具備合適備份機制？	■	□	□	
	2.3 是否完成系統弱掃，並完成修補中級(含)以上之風險？	■	□	□	由學校提供第三方弱掃報告進行修改
	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？	■	□	□	
	2.5 是否完成滲透測試，並完成修補中級(含)以上之風險？	■	□	□	
	2.6 是否完成源碼檢測，並完成修補中級(含)以上之風險？	■	□	□	
	2.7 是否實施之系統日誌管理？	■	□	□	
	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？	■	□	□	採線上演練
	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？	■	□	□	
1. 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：寶慶文化科技股份有限公司

住址：臺中市南區忠明南路580巷9號1樓

國立中央大學附屬中壢高級中學

委外廠商保密同意書

茲緣於簽署人為　寶慶文化科技股份有限公司　（廠商名稱，以下稱廠商）之負責人，本公司負責國立中央大學附屬中壢高級中學(以下稱本校)　M7圖書館自動化系統維護壹年期(114年度)　(資通業務案名，以下稱「本案」)，本案為□核心業務■非核心業務(請勾選)，於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 本校資安責任等級為□C 級 ■D 級(請勾選)。其中，核心業務安全防護等級為□高級 □中級 ■普級(請勾選)。簽署人承諾於本契約有效期間內配合資通業務責任等級及校內資安責任等級，並依各項資安法規規範，進行本案各項工作。

第二條 簽署人應主動了解本案防護等級，並遵守本校相關法令及規範，如「資通安全政策」等。

第三條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切本校未標示得對外公開之公務秘密，以及本校依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於本校指定之處所內使用之。非經本校事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本校或本校所指定處所以外之處所。

第四條 簽署人知悉或取得本校公務秘密與業務秘密應限於其執行本契約所必

需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第五條　簽署人在下述情況下解除其所應負之保密義務：

一、原負保密義務之資訊，由本校提供以前，已合法持有或已知且無保密必要者。

二、原負保密義務之資訊，依法令業已解密、依契約本校業已不負保密責任、或已為公眾所知之資訊。

三、原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第一條　簽署人若違反本同意書之規定，本校得請求簽署人及其任職之廠商賠償本校因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負連帶賠償責任。

第二條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

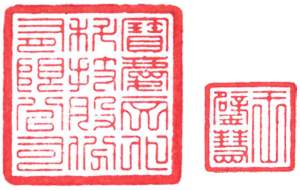
第三條　本同意書一式叁份，本校、簽署人及寶慶文化科技股份有限公司（廠商）各執存一份。

簽署廠商負責人姓名及簽章：王璧慧

簽署廠商負責人住址：臺中市南區忠明南路580巷9號1樓

聯絡電話：04-23716127

廠商名稱、住址及公司章：寶慶文化科技股份有限公司



中　華　民　國　　114　　年　　8　　月　　19　　日

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 盧彥碩、陳建瑋、陳宣行 (簽署人姓名)等，受 寶慶文化科技股份有限公司 （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） M7圖書館自動化系統維護壹年期(114年度) （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：

立切結書人所屬廠商：寶慶文化科技股份有限公司

廠商名稱及蓋章

廠商負責人姓名及簽章：王璧慧

廠商負責人聯絡電話及地址：04-23716127/臺中市南區忠明南路580巷9號1樓

中　華　民　國　　114　　年　　8　　月　　19　　日