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 07 月 03 日

委外廠商名稱	富利資訊股份有限公司	**委外廠商負責人**	郭慶龍
專案名稱	出納帳務管理系統	**單位/專案負責人**	

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____ ■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：__未指派專責人員如有需求富利可協助處理__
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：_____
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：_____ ■未就本專案範圍內之資通系統規劃安全性檢測 備註：__因系統為 AP 故無法執行弱點掃描，可提供安全性檢測證明。___
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)_防毒軟體及防火牆__(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__種等級，相關存取控制、權限管理機制說明如下： _____ □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_1_小時之資安通識教育訓練，對象包含公司全體同仁； _3_小時之資安專業教育訓練，對象包含公司全體同仁； _2_小時之個資通識教育訓練，對象包含公司全體同仁。 □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：_____

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：陳靜瑩　　填表日期：114 年 07 月 03 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？	■	□	□	資安等級為■D 級
	1.2 是否是否知悉合約標的之系統防護基準？	■	□	□	防護等級為■普級
	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？	□	□	■	合約未包含資安維護及系統防護基準之提供。
2.應辦事項	2.1 系統是否符合防護基準？	□	□	■	廠商遵守資安法。但不包含資安法所延伸之系統修改、伺服器、資料庫與網路之管理維護與防護作業等工作事項。上述工作事項由機關負責，或由機關提出需求後，經雙方討論後議定之。
	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？	□	□	■	資通安全責任等級 D、非核心系統，無需辦理系統弱掃
	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？	□	□	■	資通安全責任等級 D、非核心系統，無需辦理資通安全健診
	2.5 是否完成滲透測試，並完成修補中級(含)以上之風險？	□	□	■	資通安全責任等級 D、非核心系統，無需辦理滲透測試
	2.6 是否完成源碼檢測，並完成修補中級(含)以上之風險？	□	□	■	資通安全責任等級 D、非核心系統，無需辦理源碼檢測
	2.7 是否實施之系統日誌管理？	□	□	■	合約未包含資安維護及系統防護基準之提供。
	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？	□	□	■	(依實際演練內容、次數報價)
	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？	■	□	□	
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

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	3.2 是否簽署廠商保密同意書、廠商執行人員保密切結書	■	□	□	■執行人員保密切結書 □執行人員保密同意書
	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：富利資訊股份有限公司

新竹市香山區牛埔南路125號