113年第六次電腦軟體共同供應契約採購-雲端服務

(1130206) 雲端服務檢核表

雲端微服務（SaaS）套裝型

共通性資通安全基本要求

以下為「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表(112.9.25版)」中，要求【普】、【中】及【高】類型之資料或系統類型應建議辦理之各項控制措施。

請投件廠商依本檢核表就所提之雲端服務產品實際情形勾選為【普級】或【中】、【高】資料或系統類型，併於廠商說明欄填覆相關對應措施，本表格內容後續將公告於資訊服務採購網中。

服務名稱： Yory優歷 線上學習歷程引導教練

☑ 符合【普級】資料或系統類型(所有「高、中、普」標記●項目，皆須符合並進行說明，標記「高、中」標記●項目，則為選填)

□符合【中】、【高】資料或系統類型(所有項目皆須符合並進行說明)

填寫說明：

1. 圖示表示：● 建議辦理，◎ 經訂購機關評估個案有必要辦理時，▲ 依訂購機關機關資通安全責任等級辦理。
2. 普、中、高皆標示◎項目(橘色項目)，為所有廠商選填項目，提供機關個別評估時參考。

| 項目 | 子項 | 資料或系統類型 | | | 請廠商自我檢視並填寫相關說明  填寫日期：中華民國 113 年 8 月 15 日 |
| --- | --- | --- | --- | --- | --- |
| 高 | 中 | 普 |
| 提供服務商 | 須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準 | ● | ● | ● | ☑ 符合要求：  雲端服務應具備以下三項資訊安全管理制度及雲端服務個人資訊保護相關國際或國家標準驗證(通過驗證之證明文件須顯示出雲端服務在驗證範圍內，雲端服務原廠得以合作之公有雲業者通過驗證證書代之)：   1. 資訊安全管理系統國際標準(ISO/IEC 27001)或國家標準(CNS 27001)，二者擇一。 2. 雲端服務資訊安全管理國際標準，如ISO/IEC 27017或雲端安全聯盟CSA Star(等級不限)等，二者擇一 3. 雲端服務個人資訊保護管理國際標準(ISO/IEC 27018)。 |
| 須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準  (提供服務項目涉及個資時機關應納入要求) | ◎ | ◎ | ◎ | ☑ 符合要求 |
| 不得為大陸地區廠商或第三地區含陸資成分廠商 | ● | ● | ● | ☑符合要求：   1. 雲端服務原廠不得為「中國大陸（含港、澳）地區廠商」或「經濟部投資審議司列為陸資來台投資事業名錄之廠商」者。 2. 經數位發展部資通安全署、國家安全會議及其他資安、國安等機關通知有資安疑慮，例如投件廠商、投件代理商所提供產品之原廠屬「第三地區含陸資成分廠商」。 |
| 身分鑑別/傳輸機密性與完整性 | 廠商提供機關帳號控管措施 | ◎ | ◎ | ◎ | (為機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 廠商提供機關資料傳輸措施 | ◎ | ◎ | ◎ | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 事件日誌保存與可歸責性 | 應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求 | ● | ● | ● | 依雲端服務共契採購契約要求，雲端服務與履約標的相關之日誌保存項目如下：   1. 應用程式日誌(AP log)(必要) 2. 登入日誌(logon log)(必要) 3. 網站日誌(web log)(必要) 4. 作業系統日誌(OS event log)： 系統將記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等。   上述日誌項目保存期限：自資料產生起保存至少6個月(含契約終止或解除或期滿後)。  優歷 Yory 系統日誌保存使用 AWS CloudWatch 服務來達成，紀錄所有 Server 接收到的請求詳細資料，包含但不限於：userId、IP、request path、timestamps 等各項資料，並且保存期限為六個月（如下圖所示： Retention: 6 months） |
| 供應商及產品安全要求 | 針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險  1.供應商安全：符合以下任一條件。  (1)廠商有公開漏洞回報應變機制  (2)廠商有第三方檢測團隊執行檢測  2.產品安全：符合以下任一條件。  (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告  (2)提供經商用弱點檢測軟體未含\_\_\_等級風險之掃描報告  (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證 | ● | ● | ● | ☑符合要求：   1. 供應商(雲端服務原廠)安全   ☑漏洞回報應變機制：  1. 本系統採用 AWS Web Application Firewall (WAF) 來防護入侵、阻檔監測活動管理，根據常見的網路攻擊、滲透、漏洞攻擊等建立防護規則，用以即時阻擋不安全的連線或要求。  2.如發現有資訊安全事件 (包括但不限於廠商公司資料或採購方客戶、員工之個人資料外洩、遭棄置、非法入侵或病毒攻擊等)，將立即採取防制措施，並將即時通報採購方及協助進行相關處理程序。  3. 在 AWS WAF 功能中，依據常見的網路攻擊，建立防範規則，在 LoadBalancer 層就直接阻擋攻擊，不會讓攻擊或有害的請求進入到 Server。  以下圖為例，可以看見經由 WAF 擋下的請求數量，以及詳細內容。    若真的發生嚴重的漏洞或攻擊事件，將會自動透過 AWS 的 SNS 服務通知網站管理者，接著識別事件影響程度、範圍，若確認有用戶資料外洩的疑慮，將會主動通知相關單位。  ▢ 有第三方檢測團隊執行檢測：請提供第三方檢測團隊資訊   1. 產品安全 2. 請詳閱雲端服務安全性檢測個案編號CS-002( OWASP TOP10 最新版應用程式弱點掃描) 3. 請詳閱雲端服務安全性檢測個案編號CS-003(系統弱點掃描) 4. ▢ 本雲端服務提供App，並取得行動應用App基本資安標章。   App名稱：請填本雲端服務提供之App名稱  ▢ Android：請填版本號 ▢ iOS：請填版本號 |
| 廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC) | ◎ | ◎ | - | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 資料安全 | 未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區 | ● | ● | ● | ☑符合要求：  雲端服務資料儲存所在地於本國境內者，未經機關審查同意不得隨意變更至本國境外。 |
| 資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。 | ● | ● | ● | ☑符合要求：  雲端服務資料存取、備份及備援之實體機房所在地不得位於中國大陸（含港、澳），且不得跨該等境內傳輸相關資料。 |
| 廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明做法) |