社團法人中華民國諮商心理師公會
「諮商心理師職後支持系統線上課程平台」規格需求說明書

壹、專案概述

一、專案名稱

社團法人中華民國諮商心理師公會「諮商心理師職後支持系統線上課程平台」租用案，以下簡稱本案。

二、專案目標：建置能長久培育新一代諮商心理師的執照後二年臨床實務訓練，並且增加訓練內容對新手心理師而言之可近性（accessibility），同時使得訓練資源得以保存、定期更新及永續經營，並可獲得寶貴訓練成效的數據以提供未來政策實施策略修訂的參考。

三、專案範圍

本案內容包括

（一） 線上課程平台網頁之使用權

（二） 線上課程平台網頁之維運

四、專案時程

決標後，本會通知專案會議啟動日起，至多 90 日曆天內完成上線驗收，後續租賃履約至 115 年 12 月 31 日止。

貳、採購功能需求

響應式網頁技術（RWD）	網站應符合或相容於最新 HTML、CSS 及 JavaScript 標準，並採用 RWD 技術，確保學員使用手機、平板或桌機之網頁瀏覽器時，畫面能隨裝置尺寸自動縮放優化。
瀏覽器相容性	須確保支援各類主流瀏覽器（如 Chrome、Edge 等）之最新及前一個主要版本，確保學員在不同使用情境下皆能穩定操作。
同步與非同步教學	支援上傳各類教學資源（如文字、影音、PPT、PDF），並提供學員連結外部即時課程（如 Zoom 平台之線上課程），以達到教學資源永續。
內部課程管理	平台須提供至少 100GB 以上之儲存空間，並須保留未來擴充容量之議約可能性，供管理方上傳內部專屬課程，並具備權限控管功能。
完課與測驗機制	具備完課後線上測驗功能，並能標示已通過測驗之課程項目。另部分連結外部平台之即時課程，亦須能在平台上有完課之紀錄。
能力指標管理機制	能依據諮商心理師核心職能設計，建立不同指標對應之課程類別，並支援學習歷程紀錄（e-Portfolio）。
數據儀表板	提供管理端學習成效儀表板，即時呈現學習數據、評量

	結果與整體訓練趨勢。
標準化 API 介接	具備標準 API 介接能力，能與本會既有系統或外部資料庫串聯，並提供 API 導入相關技術文件。
報表匯出功能	支援將學習數據與評量結果轉出為 PDF、DOCX 或 XLSX 等格式之電子檔。
帳號與權限控管	採分層授權機制，且至少包含全域管理、教師、學員三層。另應提供存取控制管理，包含授予和取消帳號權限，以及定期進行權限清查，移除不必要的權限授予。
身分驗證安全性	系統須具備自動斷線機制（如閒置逾 15-30 分鐘），密碼不得以明文存放，且須符合複雜度要求。
資通安全規範	傳輸須採用 HTTPS（TLS 1.2 以上），敏感資料應進行加密儲存，並於上線前通過弱點掃描。資通系統防護基準評估詳見附件一。
服務水準協定 (SLA)	廠商須承諾系統穩定性，若發生問題應於指定時間內協助排除，並定期提交維運或保固報告。

本規格所述功能與技術內容，係描述本案線上課程系統之必要能力，投標相同或優於本規格功能之解決方案，不以特定產品、資料庫或實作架構為限。

參、導入期服務

一、線上會議及教育訓練：廠商應提供至少 1 次線上教育訓練予本會相關人員。

二、廠商應提供系統操作手冊或說明書。

肆、服務期間之維運與支援

一、合約期限內本會擁有平台之使用權。合約期滿廠商收回平台之相關程式與權限。

二、廠商提供平台之偵錯與維護，以維持其正常運作，並協助本會於操作本系統時的異常問題排除。

伍、驗收與付款

一、履約期限：租賃至 115 年 12 月 31 日止。

二、付款方式：驗收完成後辦理一次性付款。

三、驗收條件：符合需求所列之事項。

附件一、資通系統防護基準評估表

編號	構面	措施內容	高	中	普	控制措施	對應措施
1.	存取控制	帳號管理			●	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	
2.	存取控制	帳號管理			●	定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	
3.	存取控制	帳號管理			●	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及 條件。	
4.	存取控制	帳號管理			●	逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。	
5.	存取控制	帳號管理			●	應依機關規定之情況及條件，使用資通系統。	
6.	存取控制	帳號管理			●	監控資通系統帳號，如發現帳號違常使用時回報管理者。	
7.	存取控制	遠端存取			●	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	
8.	存取控制	遠端存取			●	使用者之權限檢查作業應於伺服器端完成。	
9.	存取控制	遠端存取			●	應監控遠端存取機關內部網段或資通系統後臺之連線。	
10.	存取控制	遠端存取			●	應採用加密機制。	
11.	存取控制	遠端存取			●	遠端存取之來源應為機關已預先定義及管理之存取	

編號	構面	措施內容	高	中	普	控制措施	對應措施
						控制點。	
12.	事件日誌與可歸責性	記錄事件			●	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	
13.	事件日誌與可歸責性	記錄事件			●	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	
14.	事件日誌與可歸責性	記錄事件			●	應記錄資通系統管理者帳號所執行之各項功能。	
15.	事件日誌與可歸責性	記錄事件			●	應定期審查機關所保留資通系統產 生之日誌。	
16.	事件日誌與可歸責性	日誌紀錄內容			●	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	
17.	事件日誌與可歸責性	時戳及校時			●	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)。	
18.	事件日誌與可歸責性	時戳及校時			●	系統內部時鐘應定期與基準時間源進行同步。	
19.	事件日誌與可歸責性	日誌資訊之保護			●	對日誌之存取管理，僅限於有權之使用者。	
20.	事件日誌與可歸責性	日誌資訊之保護			●	應運用雜湊或其他適當方式之完整性確保機制。	

編號	構面	措施內容	高	中	普	控制措施	對應措施
21.	事件日誌與可歸責性	日誌資訊之保護			●	定期備份日誌至原系統外之其他實體系統。	
22.	營運持續計畫	系統備份			●	訂定系統可容忍資料損失之時間要求。	
23.	營運持續計畫	系統備份			●	執行系統源碼與資料備份。	
24.	營運持續計畫	系統備份			●	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	
25.	營運持續計畫	系統備份			●	應將備份還原，作為營運持續計畫測試之一部分。	
26.	營運持續計畫	系統備份			●	應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	
27.	營運持續計畫	系統備援			●	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	
28.	營運持續計畫	系統備援			●	原服務中斷時，於可容忍時間內，由 備援設備或其他方式取代並提供服 務。	
29.	識別與鑑別	內部使用者之識別與鑑別			●	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	
30.	識別與鑑別	內部使用者之識別與鑑別			●	對帳號之網路或本機存取採取多重認證技術。	
31.	識別與鑑別	身分驗證管理			●	使用預設密碼登入系統時，應於登入後要求立即變更。	
32.	識別與鑑別	身分驗證管理			●	身分驗證相關資訊不以明文傳輸。	

編號	構面	措施內容	高	中	普	控制措施	對應措施
33.	識別與鑑別	身分驗證管理			●	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	
34.	識別與鑑別	身分驗證管理			●	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	
35.	識別與鑑別	身分驗證管理			●	使用者更換密碼時，至少不可以與前三次使用過之密碼相同。(非內部使用者，依本會規範辦理)	
36.	識別與鑑別	身分驗證管理			●	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	
37.	識別與鑑別	身分驗證管理			●	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	
38.	識別與鑑別	鑑別資訊回饋			●	資通系統應遮蔽鑑別過程中之資訊。	
39.	識別與鑑別	加密模組鑑別			●	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	
40.	識別與鑑別	非內部使用者之識別與鑑別			●	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)。	
41.	系統與服務獲得	系統發展生命週期需求階段			●	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	

編號	構面	措施內容	高	中	普	控制措施	對應措施
42.	系統與服務獲得	系統發展生命週期設計階段			●	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	
43.	系統與服務獲得	系統發展生命週期設計階段			●	將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	
44.	系統與服務獲得	系統發展生命週期開發階段			●	應針對安全需求實作必要控制措施。	
45.	系統與服務獲得	系統發展生命週期開發階段			●	應注意避免軟體常見漏洞及實作必要控制措施。	
46.	系統與服務獲得	系統發展生命週期開發階段			●	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	
47.	系統與服務獲得	系統發展生命週期開發階段			●	執行「源碼掃描」安全檢測。	
48.	系統與服務獲得	系統發展生命週期開發階段			●	具備系統嚴重錯誤之通知機制。	
49.	系統與服務獲得	系統發展生命週期測試階段			●	執行「弱點掃描」安全檢測。	
50.	系統與服務獲得	系統發展生命週期測試階段			●	執行「滲透測試」安全檢測。	
51.	系統與服務獲得	系統發展生命週期部署與維運階段			●	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	
52.	系統與服務獲得	系統發展生命週期部署與維運階段			●	資通系統相關軟體，不使用預設密碼。	

編號	構面	措施內容	高	中	普	控制措施	對應措施
53.	系統與服務獲得	系統發展生命週期部署與維運階段			●	於系統發展生命週期之維運階段，須注意版本控制與變更管理。	
54.	系統與服務獲得	系統發展生命週期委外階段			●	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	
55.	系統與服務獲得	獲得程序			●	開發、測試及正式作業環境應為區隔。	
56.	系統與服務獲得	系統文件			●	應儲存與管理系統發展生命週期之相關文件。	
57.	系統與通訊保護	傳輸之機密性與完整性			●	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	
58.	系統與通訊保護	傳輸之機密性與完整性			●	使用公開、國際機構驗證且未遭破解的演算法。	
59.	系統與通訊保護	傳輸之機密性與完整性			●	使用演算法支援的最小長度金鑰。	
60.	系統與通訊保護	傳輸之機密性與完整性			●	加密金鑰或憑證週期性更換。	
61.	系統與通訊保護	傳輸之機密性與完整性			●	伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	
62.	系統與通訊保護	資料儲存之安全			●	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方	

編號	構面	措施內容	高	中	普	控制措施	對應措施
						式儲存。	
63.	系統與資訊完整性	漏洞修復			●	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	
64.	系統與資訊完整性	漏洞修復			●	定期確認資通系統相關漏洞修復之狀態。	
65.	系統與資訊完整性	資通系統監控			●	發現資通系統有被入侵跡象時，應通報機關特定人員。	
66.	系統與資訊完整性	資通系統監控			●	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	
67.	系統與資訊完整性	資通系統監控			●	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	
68.	系統與資訊完整性	軟體及資訊完整性			●	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	
69.	系統與資訊完整性	軟體及資訊完整性			●	使用者輸入資料合法性檢查應置放於應用系統伺服器。	
70.	系統與資訊完整性	軟體及資訊完整性			●	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	
71.	系統與資訊完整性	軟體及資訊完整性			●	應定期執行軟體與資訊完整性檢查。	