

財團法人台灣設計研究院

「教科書設計獎網站資安規劃及維護」採購案(案號 : 1151003542)
徵求建議書

一、 企劃書規格包含下列：

- (一) 依規格需求提供建議書，採用 A4 紙張，橫書雙面列印或簡報資料。
- (二) 團隊介紹：含相關專業背景介紹、業務經驗等，並請提供開發與維運能力說明。
- (三) 資安證照：專案負責人或專案經理(PM)須具備 ISO 27001:2022 資安管理相關證照；投標公司須持有有效之 ISO 27001:2022 驗證證書。
- (四) 請參考附件 1-1 資通系統防護基準表控制項，說明後續規劃及控制措施。
- (五) 報價單。

二、 交付份數：一式【4 份】。

三、 背景說明

「教科書設計獎」旨在鼓勵教科書出版及設計相關單位，從內容、編輯、視覺設計、使用者需求及教育應用等面向持續創新，提升教科書的整體設計品質與閱讀體驗。透過獎項的推動，除了肯定優秀的教科書設計成果，也期望促進教育、出版與設計等不同領域之間的交流，進一步發掘具創新性、實用性及教育價值的優良作品。

其官方網站為獎項對外溝通與服務的重要數位平台，除提供獎項相關資訊外，亦涵蓋徵件、報名、獲獎作品、評選資訊及得獎成果等多元應用，肩負參賽單位、評審、一般民眾及相關教育與出版單位之資訊服務需求。

因此，網站維護工作除確保網站正常運作外，亦應配合獎項執行期程，

財團法人台灣設計研究院

持續進行網站內容更新、功能維護、使用者體驗優化、系統安全及網站效能管理，並因應不同年度徵件及評選需求進行必要的功能調整，使網站能穩定支援獎項各階段業務，並持續發揮教科書設計獎之資訊傳播、作品展示及成果推廣功能。

四、 預算金額：新臺幣 750,000 元整 (含稅)

五、 履約期程：決標次日起至 115 年 12 月 15 日止

六、 規格需求

項目	項次	需求說明
網站	1	「示範成果頁」與「得獎作品頁」調整及切版設計
	2	報名 ICON 設計與調整
	3	整站顯示名稱及預覽圖示調整
	4	網站社群成效追蹤碼設定及串接
	5	Footer 設計切版與調整
	6	首頁新增合作單位區塊，包含分類及網址超連結
系統	7	網站軟體核心升級 rails 6.1.4 升級至 rails 8 以上版本
	8	資安弱點掃描，包含初掃及複掃，並修復掃出之所有風險弱點

財團法人台灣設計研究院

項目	項次	需求說明
	9	網站及資安普級維護，依據附件 1-1 之檢核項目文件，處理「普」級所須事項。

七、 本案聯絡人

(一)有關本採購案比稿內容之諮詢，請洽 02-2745-8199 分機 383 林先生。

(二)採購事宜聯繫窗口:02-2745-8199 分機 106 許小姐;分機 212 潘小姐。

八、 投標：郵寄時請於郵件封套上註明**投標廠商名稱、地址、「教科書設計獎網站資安規劃及維護」**，送達台灣設計研究院採購工作小組收(11072 台北市光復南路 133 號)；專人送達請送至本院服務台。以上送達方式皆須依招標公告之**截止收件期限(下午 17:00) 前送達**，逾期恕不受理，如有延誤應自行負責。

附件 1-1 資通系統防護基準表

編號	安全類型	措施內容	系統防護需求	普	中	高
01	存取控制	帳號管理	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	★	★	★
02	存取控制	帳號管理	已逾期之臨時或緊急帳號應刪除或禁用。		★	★
03	存取控制	帳號管理	資通系統閒置帳號應禁用。		★	★
04	存取控制	帳號管理	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。		★	★
05	存取控制	帳號管理	機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。			★
06	存取控制	帳號管理	逾越機關所許可之間置時間或可使用期限時，系統應自動將使用者登出。			★
07	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。			★
08	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。			★
09	存取控制	最小權限	採最小權限原則，僅允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。		★	★
10	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。	★	★	★
11	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。	★	★	★
12	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。	★	★	★
13	存取控制	遠端存取	應採用加密機制。	★	★	★
14	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控制點。(系統(網站)請以現場維護、至委辦單位辦公場所、或至本署資訊室核備地點連線至計畫網站辦理維護。)	★	★	★
15	事件日誌	紀錄事件	訂定日誌之記錄時間週期及留存政策，並保留日誌	★	★	★

財團法人台灣設計研究院

	與可歸責性		至少六個月。			
16	事件日誌與可歸責性	紀錄事件	確保資通系統有紀錄特定事件之功能，並決定應紀錄之特定資通系統事件。	★	★	★
17	事件日誌與可歸責性	紀錄事件	應記錄資通系統管理者帳號所執行之各項功能。	★	★	★
18	事件日誌與可歸責性	日誌事件	應定期審查機關所保留資通系統產生之日誌。		★	★
19	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，並採用單一日誌紀錄機制，確保輸出格式的一致性，並應依資通安全政策及法規要求納入其他相關資訊。	★	★	★
20	事件日誌與可歸責性	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。	★	★	★
21	事件日誌與可歸責性	日誌處理失效之回應	資通系統於日誌處理失效時，應採取適當之行動。	★	★	★
22	事件日誌與可歸責性	日誌處理失效之回應時戳及校時	機關規定需要即時通報之日誌失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。			★
23	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，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	★	★	★
24	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。		★	★

財團法人台灣設計研究院

	性					
25	事件日誌 與可歸責 性	日誌資訊 之保護	對日誌之存取管理，僅限於有權限之使用者。	★	★	★
26	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。		★	★
27	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。			★
28	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。	★	★	★
29	營運持續 計畫	系統備份	執行系統源碼與資料備份。	★	★	★
30	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。		★	★
31	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。			★
32	營運持續 計畫	系統備份	應在與運作系統不同地點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。			★
33	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。		★	★
34	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。		★	★
35	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。	★	★	★
36	識別與鑑 別	內部使用 者之識別 與鑑別	對資通系統之存取採取多重認證技術。			★

財團法人台灣設計研究院

37	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。	★	★	★
38	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。	★	★	★
39	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。	★	★	★
40	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。	★	★	★
41	識別與鑑別	身分驗證管理	密碼變更時，至少不可以與前三次使用過的密碼相同。	★	★	★
42	識別與鑑別	身分驗證管理	對非內部使用者，可依機關自行規範密碼設定強度、效期與密碼不重複次數。	★	★	★
43	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。		★	★
44	識別與鑑別	身分驗證管理	密碼重設機制對使用者新身分確認後，發送一次性及具有時效符記。		★	★
45	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。	★	★	★
46	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。		★	★
47	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之程序）。	★	★	★
48	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）進行確認。	★	★	★
49	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。		★	★

財團法人台灣設計研究院

50	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。		★	★
51	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。	★	★	★
52	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。	★	★	★
53	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，不包含詳細之錯誤訊息。	★	★	★
54	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。			★
55	系統與服務獲得	系統發展生命週期開發階段	系統應具備發生嚴重錯誤時之通知機制。			★
56	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。	★	★	★
57	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。			★
58	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。	★	★	★
59	系統與服務獲得	系統發展生命週期部署與維	資通系統不使用預設密碼。	★	★	★

財團法人台灣設計研究院

		運階段				
60	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，應執行版本控制與變更管理。(原始程式庫新增、修改、修改存取是否有控制措施並留有稽核日誌記錄存取行為)	★	★	★
61	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、可用完整）納入委外契約。	★	★	★
62	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。		★	★
63	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。	★	★	★
64	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。			★
65	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之演算法。			★
66	系統與通訊保護	傳輸之機密性與完整性	支援演算法最大長度金鑰。			★
67	系統與通訊保護	傳輸之機密性與完整性	加密金鑰或憑證應定期更換。			★
68	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。			★
69	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式儲存。			★
70	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。	★	★	★

財團法人台灣設計研究院

71	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。		★	★
72	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。	★	★	★
73	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。		★	★
74	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。			★
75	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。		★	★
76	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端。		★	★
77	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。		★	★
78	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。			★