



實踐大學

115 年度全校資訊安全管理制度建置輔導案

（台北、高雄校區）

需求說明書

專案時程：自決標日起至 115 年 12 月 18 日

壹、專案說明

一、專案名稱

實踐大學（以下簡稱本校）115 年度全校資訊安全管理制度建置輔導案(北高校區)（以下簡稱本專案）。

二、專案目標

協助本校之相關資訊業務，提供資訊安全管理制度建置與維護輔導服務，以符合教育部與「大專校院高等教育深耕計畫資安強化專章」要求之項目。

三、專案範圍

- (一)協助本校完成資訊安全管理制度建置輔導作業，115 年度預計導入 3 個教學單位(管理學院、商資學院、國際學程，以下簡稱導入單位)，進行資訊資產盤點、風險評估作業。
- (二)協助本校 112-114 年度已導入之 11 個行政單位(秘書室、教務處、總務處、學務處、研發處、人資處、財務處、入學服務處、共同課程委員會、國際事務處、推廣教育部)與 2 個教學單位(民生學院、文創學院)，進行資訊資產盤點、風險評估檢視、諮詢作業。
- (三)協助調整與修訂本校現有之資訊安全管理制度程序文件內容。
- (四)提供本校導入單位資訊安全管理制度建置導入教育訓練課程與諮詢服務。
- (五)提供本校導入單位之資訊安全管理制度之內部稽核活動。
- (六)協助執行本校導入單位之個人電腦安全性檢測作業。
- (七)協助執行本校圖書資訊處資安技術檢測作業。

- (八)協助本校圖書資訊處完成資訊安全管理制度 ISO 27001:2022
第三方驗證作業。

四、專案時程

自決標日起至 115 年 12 月 18 日。

貳、專案需求

一、資訊安全管理制度(ISMS)

- (一)協助將本校現有資訊安全管理制度程序書、表單等文件修訂。
- (二)協助本校導入單位執行鑑別及評價資訊資產作業。
- (三)協助本校導入單位執行風險評鑑作業。
- (四)協助本校導入單位執行風險處理作業。
- (五)規劃及執行本校導入單位資訊安全內部稽核作業。
- (六)協助本校導入單位內部稽核發現事項矯正措施、改善與建議作業。
- (七)ISMS 資訊安全管理及資安法令宣導。
- (八)ISMS 資訊安全管理制度文件宣導。
- (九)其他資訊安全相關問題諮詢及建議。

二、教育訓練

專案執行期間，協助辦理主管教育訓練課程與一般人員教育訓練課程，並應配合管理系統導入工作事項，規劃與實施資訊安全教育訓練，安排講師並提供教材，各項教育訓練需求場數與時數至少如下：

主管教育訓練課程 1.5 小時、一般人員教育訓練課程北高各 1.5 小時，資訊安全建置導入教育訓練北高各 8 小時：

項次	課程內容	場次	每場次時數
1	資訊資產盤點課程	1	2 小時
2	資訊安全風險評鑑及管理方法	1	2 小時
3	營運持續管理	1	2 小時
4	資訊安全稽核重點說明暨文件宣導課程	1	2 小時

三、技術檢測作業

(一)由得標廠商協助，協助執行圖書資訊處資安技術檢測作業，以及導入單位之個人電腦安全性檢測作業。

包括：

1、網站(Web)滲透測試

由得標廠商透過工具（由廠商自備），以遠端連線方式，協助本校圖書資訊處進行所提供之網站 IP 測試服務。

2、網站主機弱掃

協助本校圖書資訊處進行所提供之網站範圍，針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合 Common Vulnerabilities and Exposures (CVE)發布的弱點內容。

3、使用者端電腦檢視（圖書資訊處及導入單位）。

(二)檢視掃描分析完畢後，提供檢測服務報告。

四、ISO 27001:2022 第三方驗證作業服務

(一)協助本校圖書資訊處第三方驗證機構驗證前準備作業，包含驗證機構聯繫申請、驗證前之文件整備作業。

(二)陪同進行第三方驗證機構驗證作業與驗證發現改善作業。

參、管理需求

一、專案計畫

(一)簽約次日起 1 個月內交付專案工作計畫書，經本校同意後據以實施。

(二)專案人力

專案經理須具 ISO 27001 LA、ISO 27701、BS 10012 LA 全數專業證照，主要工作人員須具 ISO 27001 LA、ISO 27701、BS 10012 LA 專業證照至少 1 種。專案期間，人員更換除離職外，須經本校同意或本校提出更換要求時，始得更換。

(三)顧問到點輔導之時數要求

台北校區

- 1、導入期間至少到點輔導 6 人天（不含內部稽核作業），每次至少 4 小時（0.5 人天計）。
- 2、專案期間之顧問到點輔導時數，以會議紀錄為其佐證資料。
- 3、內部稽核作業至少人 4 人天。

高雄校區

- 1、導入期間至少到點輔導 5 人天（不含內部稽核作業），每次至少為 1 人天（併同教育訓練課程辦理時，可以 0.5 天計）。
- 2、專案期間之顧問到點輔導時數，以會議紀錄為其佐證資料。
- 3、內部稽核作業至少人 2 人天。

二、資訊安全

(一)廠商維護本專案所獲得之資訊，應依個人資料保護法及相關法令之規定恪遵保密原則，並應簽署「承包廠商保密同

意書」，如有違失，廠商須負相關法律責任及實質賠償損害責任。

(二)廠商應遵守本校資訊安全政策暨相關規定，如有違失造成本校發生資訊安全事件時，廠商須負實質賠償損害責任。

肆、交付項目及付款條件

交付項目、付款條件及付款比例(分 2 期付款)如下表：

交付日期	交付項目、付款條件及付款比例	
第 1 期 (簽約次日起 1 個月內)	交付項目	(1)專案工作計畫書
	付款比例	契約價金 20%
第 2 期 (簽約次日起 至 115 年 12 月 18 日)	交付項目	(2)資訊資產清單
		(3)風險評鑑報告
		(4)內部稽核報告
		(5)第三方驗證稽核報告
		(6)ISO 27001:2022 證書持續有效證明函
		(7)教育訓練教材
		(8)技術檢測報告
		(9)資訊安全管理制度程序文件（電子檔）
	付款比例	契約價金 80%

一、其他下列執行過程之交付/協助完成項目，均以電子檔提供予本校承辦人員留存。專案各時程交付項目如下表所示：

活動項目	交付/協助完成項目	形式	交付時機
啟動準備	1.啟動會議簡報資料 2.工作計畫書	交付	專案執行開始 1 個月內
資訊安全資訊資產盤點與風險評鑑活動	1.資訊資產清冊 2.風險評鑑報告 3.風險處理計畫	協助完成	115/9/30 前
檢視/修訂資訊安全四階文件	修訂後之 ISMS 文件	協助完成	115/10/16 前
技術檢測	滲透測試與弱點掃描技術檢測結果報告(含導入單位個人電腦安全性檢測)	交付	115/10/31 前
內部稽核	1.內部稽核計畫 2.內部稽核報告 3.改善計畫或矯正措施表	交付	115/10/31 前
ISO 27001:2022 第三方驗證作業	ISO 27001:2022 證書持續有效證明函	交付	115/12/19 前
資訊安全教育訓練	各階段訓練課程講義	交付	訓練前 1 週內

二、本專案要求交付之報告、計畫等各項文件，須交付書面及光碟各 1 份，均須經本校確認。