

「設計導向 AI 知識基礎建置及驗證」採購案契約書

契約編號：1151003758

執行期間：自民國 000 年 00 月 00 日起
至民國 115 年 12 月 15 日止
(保固期間為上線後一年)

甲 方：財團法人台灣設計研究院
乙 方：

中華民國 年 00 月 00 日

「設計導向 AI 知識基礎建置及驗證」採購案契約書

立約人：財團法人台灣設計研究院（以下稱甲方）
OOOOO（以下稱乙方）

緣甲方委託乙方提供本契約之採購標的，雙方同意訂定本契約，以資共同遵守，其條款如下：

第一條 契約範圍

- 1、 乙方之執行範圍包括本契約條款及相關附件：
 - (1) 「設計導向 AI 知識基礎建置及驗證」採購案需求說明書（含驗收規範）、
 - (2) 資通系統防護需求分級評估表
 - (3) 「設計導向 AI 知識基礎建置及驗證」資通系統管理暨自我檢核表、
 - (4) 本案參與人員組織表、
 - (5) 資料返還切結書、
 - (6) 資訊安全暨個資保密同意書、
 - (7) 本案服務水準協議（SLA）指標、
 - (8) 報價單。
- 2、 本契約與其附件之變更或補充，均視同本契約之一部，其效力與本契約相同；惟若與本契約抵觸時，仍以本契約條款為準。
- 3、 本案辦理事項：乙方於專案執行過程中需要甲方提供行政支援時，應盡力協助。
- 4、 附件保密同意書暨利益迴避聲明應於簽約時繳回，後續如有修正調整隨時告知甲方抽換。

第二條 履約地點

甲方指定之地點。

第三條 履約期間

- 1、 中華民國（以下同）115 年 00 月 00 日起至 115 年 12 月 15 日止之期間內履行採購標的之供應；本契約執行期間，星期例假日、國定假日或其他休息日均計入。
- 2、 保固期間為正式對外上線後一年。

第三條 本契約工作內容

- 1、 本案工作內容除本契約第一條規定外，其詳如報價單所載。
- 2、 維護服務；乙方於契約期間內應提供下列各項維護服務，本契約之維護時段為星期一至星期五，以及甲方之彈性上班日（以政府或公告者為準），乙方應備有行動電話以供甲方聯絡。有關異常或故障維修之維護時段，係指甲方通知乙方之時間，乙方須依規定時間到達並開始維修，修復時間則不以維護時段為限，亦即甲方得於維護時段內隨時通知乙方進行異常或故障維修，乙方進行異常或故障維修倘逾維護時段，應繼續進行至完全修復為止，且不得另行計費。
- 3、 故障維修服務；本契約標的於維護期間內發生異常或故障時，甲方得於維護時段內通知乙方，乙方須在接獲甲方通知後 2 小時內到達（倘維修地點在甲方異地備援機房者，乙方須在接獲甲方通知後 4 小時內到達），並於到達後 4 小時內修復。倘評估無法於 4 小時內修復者，乙方應立即提供同等（或較優）設備免費供甲方使用。乙方應於修復完成後將維護標的返還甲方，並將異常或故障發生原因以書面告知甲方。如維護標的無法修復或原廠不再提供維修服務時，乙方應提供同等設備（其相關配備及條件與原維護標的相同或較優）並移轉所有權予甲方，以取代原維護標的物之修復及返還，惟因不可抗力或可歸責於甲方之事由致標的物無法即時回復正常運作，延誤之時數應予扣除。
- 4、 系統調校服務；乙方應依甲方系統實際環境需求，以書面或電子郵件提出系統調校建議，經甲方同意後，乙方須依甲方指定時間（不以維護時段為限）到達辦理系統調校服務。

- 5、 安裝修補程式服務；乙方每季應主動以書面或電子郵件提出安裝修補程式與甲方現行版本評估，經甲方同意後，乙方須依甲方指定時間（不以維護時段為限）到達辦理安裝修補程式之服務。
- 6、 問題諮詢服務；乙方於維護時段內接獲甲方通知後，須提供本契約標的相關問題諮詢服務及處理。
- 7、 系統演練測試作業；維護期間內，經甲方事前通知，乙方應配合甲方每年最多 2 次之「營運持續演練作業」，依甲方指定時間（不以維護時段為限）指派維護人員配合到場待命，免費提供必要之協助或解決軟硬體問題之支援服務。

第四條 驗收

乙方於完成各項工作後製作驗收資料，資料應依據契約第一條第一項所述內容項目相互勾稽，並派員會同驗收及簽核，以為憑據。

第五條 契約價款

本契約經雙方議價訂定為新臺幣 xxx,xxx,xxx 元整(含稅)。

第六條 付款方式

本契約依下列約定辦理付款：本契約簽定後，甲方分兩期撥付款項：

- (1) 本契約簽定後，由甲方憑乙方開立之合法憑證撥付本案經費總價 xx%，計新臺幣 xxx,xxx,xxx 元整（含稅）。
- (2) 乙方須於 115 年 12 月 15 日前完成報價單所列之所有工作內容，經甲方審核認可後，由甲方憑乙方開立之合法憑證撥付本案經費總價 xx%，計新臺幣 xxx,xxx,xxx 元整（含稅）。

第七條 品質保證

- (1) 乙方保證具有豐富之經驗及充分之能力承攬本契約之維護工作，其參與維護工作之人員亦皆具充分之經驗與能力及專業證照。
- (2) 就維護工作之履行，乙方應盡善良管理人之注意方仍應依本契約規定履行保密義務。
- (3) 乙方應要求其受任人、受僱人、代理人、協助保固之原廠及其他相關人員（下稱「參與人員」）遵守前二項規定。
- (4) 本案服務水準協議（SLA）指標詳附件。

第八條 本案智慧財產權之歸屬與權益

- 1、 乙方因履行本契約所完成之著作，應以下列方式將著作財產權於著作完成時讓與甲方，並承諾對甲方不行使著作人格權：
 - (1) 該著作係乙方所完成者，以乙方為著作人，著作財產權歸甲方所有。
 - (2) 該著作係乙方之受雇人職務上所完成者，乙方應與其受雇人約定由乙方為著作人，並由乙方將著作財產權讓與甲方。
 - (3) 該著作係乙方之受聘人所完成而其受聘人為自然人者，乙方應予該受聘人約定，由乙方為著作人，乙方並應將著作財產權讓與甲方。
 - (4) 該著作係乙方之受聘人所完成而其受聘人為法人者，乙方應予該受聘人約定，由該法人與其受雇人或受聘人約定由法人為著作人，並將其著作財產權讓與甲方。
- 2、 乙方履約結果涉及產生著作權以外之智慧財產權者，甲方享有該智慧財產權之全部權利；非經甲方書面同意，乙方不得為任何形式之複製或主張。
- 3、 乙方保證本案相關成果皆未侵犯他人智慧財產權（包括但不限於著作權、專利權、商標權與營業秘密）或其他法律上權利。若因故意或過失不法侵害他人（含國內外自然人及法人）之權利，由乙方自負法律責任，若有第三人向甲方或 OO 部提出侵權主張，乙方應立即出面解決，其產生之訴訟費用、律師費用及其他相關費用，悉由乙方負責；若因此造成甲方或 OO 部直接或間接（包括但不限於名譽）損害，乙方亦應無條件負擔賠償責任。

第七條 保密義務

- 1、 本條所稱應保密文件及資料，係指：
 - (1) 任一方在業務上定義為密、極密之一切文件及資料，包括與其業務有關之內容，任一方因執行本案而知悉或持有他方任何資料、文件。

- (2) 依法令須保密或受保護之文件及資料，例如個人資料保護法所規定者。
- 2、 本條所稱接收方，係指接受資訊之一方；揭露方則為提供或揭露機密資訊之一方。接收方於本契約中非經揭露方事前書面同意，不得揭露任何保密文件及資料予本契約無關之他方。
- 3、 接收方及其工作人員對於前項保密文件及資料，均應善盡保密責任，不得公開宣布或揭露予與本契約之履行無關之他人；接收方因履行本契約而須將本契約內容或因履行本契約而取得之應保密文件及資料揭露予他人時，應以該他人與履約有關，且揭露之內容應為該他人確有必要知悉者為限。
- 4、 接收方應保證其執行本契約之人員，包括但不限於其受僱人、受任人等，受本條之拘束。若接收方違反本條之規定，被揭露方得不經催告逕行終止本契約，並向接收方要求相當於本案經費 3 倍之懲罰性違約金及相關損害。接收方之工作人員違約，亦視同接收方違約。
- 5、 接收方因執行本契約需要，而蒐集、處理或利用他人之個人資料，應符合個人資料保護法及其他相關法令規範，若有違反，致他人之個人資料遭不法蒐集、處理、利用或其他侵害情事者，接收方應負損害賠償責任。
- 6、 接收方在下述情況下解除其依本條所應負之保密義務：
- (1) 接收方原負保密義務之資訊，已為接收方所合法持有或已知且無保密必要者。
- (2) 接收方原負保密義務之資訊，依法令業已解密、依契約業已不負保密責任、或已為公眾所週知之資訊。

- (3) 接收方原負保密義務之資訊，係接收方自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第八條 禁止轉讓

甲乙雙方於本契約中之權利義務，非經雙方書面同意，不得轉讓予任何第三人。

第九條 違約處理

一、乙方如有違約金、損害賠償、或其他任何依本契約應支付之金額；或有履約標的損壞或短缺、不實行為、未完全履約、不符契約規定、溢領經費或減少履約事項等情形時，甲方得自應付之本案經費總價中扣抵；其有不足者，經甲方通知，乙方應於接獲通知後 30 日內給付。乙方如有偽造、變造、隱匿等不實行為者，甲方除得解除或終止本契約外，得另請求相當於本案經費總價 10% 之懲罰性違約金。

二、乙方履約有下列情形之一者，甲方得暫停給付契約價金至情形消滅為止：

- (一) 履約實際進度因可歸責於乙方之事由，落後預定進度者。
- (二) 履約有瑕疵經書面通知改善而逾期未改善者。
- (三) 未履行契約應辦事項，經通知仍延不履行者。
- (四) 乙方履約人員不適任，經通知更換仍延不辦理者。
- (五) 其他違反法令或契約情形。

三、乙方履約結果如經甲方審核有瑕疵且可限期完成改善者，甲方得要求乙方限期改正，乙方應於接獲甲方通知後自費予以修正或重做。限期改正期間逾本契約期間者，仍視為逾期，依本契約第十條第一項規定計算逾期違約金。

四、乙方無法於期限內改正、拒絕改正或不能改正者，甲方得採行下列措施之一：

- (一) 自行或使第三人改正，並得向乙方請求償還改正之必要費用。
- (二) 終止或解除本契約或減少本契約價金。

五、因可歸責於乙方之事由，致履約有瑕疵者，甲方除依前二項規定辦理外，並得向乙方請求損害賠償。

第十條 遲延履約

- 1、 逾期違約金，以日為單位，乙方如未依照本契約規定期限內完成全部工作，應按逾期日數，每日依本案經費 0.1%計算逾期違約金。但未完成履約之部分不影響其他已完成部分之使用者，得按未完成履約部分之契約價金，每日依其 0.1%計算逾期違約金。逾期違約金之總額(含逾期未改正之違約金)，以本案經費 20%為上限。
- 2、 甲方及乙方因天災或事變等不可抗力或不可歸責於雙方當事人之事由，致未能依時履約者，得展延履約期限；不能履約者，得免除本契約責任。
- 3、 前項不可抗力或不可歸責事由發生或結束後，其屬可繼續履約之情形者，應繼續履約，並採行必要措施以降低其所造成之不利影響或損害。
- 4、 主張不可抗力或不可歸責事由之一方，應於事件發生及結束後 30 日內立即檢具事證，以書面通知他方，逾期不為通知者，不得據以主張展延履約期限及免除契約責任。不能履約期間逾 90 日者，任一方均得終止本契約，並準用第十一條第二項及第三項之規定。

第十一條 契約終止、解除及暫停執行

1、 乙方有下列情形之一者，甲方除得通知乙方暫停執行並停止支付相關本契約價金外，並得不經定期催告逕以書面解除本契約，於本契約解除後，就已撥付給乙方之本契約價金，除經甲方書面同意就該契約價金之全部或一部得不予返還予甲方外，乙方應於接獲甲方書面通知之日起 30 日內返還甲方，甲方如有損害並得請求損害賠償，且不補償乙方因此所生之損失：

- (1) 因可歸責於乙方之原因停止執行本契約，或乙方遲誤工作，致其進度落後，經甲方通知限期改善，仍不改善、未改善或改善未符預定進度者。
- (2) 執行內容與乙方依本契約所定應給付之標的及工作事項或其他雙方所同意之計畫或約定不符，且經甲方通知限期改善，仍不改善、未改善或改善仍不符合通知者。
- (3) 違反本契約第八條禁止轉讓之規定者。
- (4) 因可歸責於乙方之事由，致延誤履約期限，情節重大者。
- (5) 偽造或變造契約或履約相關文件，經查明屬實者。
- (6) 乙方對甲方人員或與甲方合作乙方之受雇人、受聘人、代理人或履行輔助人給予期約、賄賂、佣金、比例金、仲介費、後謝金、回扣、餽贈、招待或其他不正利益者；有其他法定終止或解除事由者。。
- (7) 無正當理由而不履行契約者。
- (8) 就本契約之完成，經甲方審查不合格，經甲方通知限期改善，仍不改善、未改善或改善後仍不合格者。

- (9) 有破產或其他重大情事，致無法繼續履約者。
- (10) 乙方未依契約規定履約，或未按規劃內容完成本案工作，自接獲甲方書面通知之次日起 10 日內或書面通知所載較長期限內，仍未改善者。
- 2、 前項情形甲方得不解除本契約，而僅終止本契約，於本契約終止後，甲方得對乙方已完成合於給付標的及工作事項或甲方要求之部分，按已完成工作之比例核算應支之費用予以結案，但乙方應先將本契約終止前所應完成之工作成果交付及轉讓給甲方。因履約瑕疵致終止本契約者亦同。
- 3、 於本契約解除或終止後 30 日內，已產生之工作成果應由乙方無償移轉給甲方。乙方逾期不為移轉者，應給付甲方每日以本案經費總價 1% 計算之懲罰性違約金，直至移轉完成為止。因可歸責於乙方事由，致甲方解除或終止本契約者，乙方應賠償甲方因此所受之直接及間接損害。
- 4、 因前述原因甲方得於一個月前以書面通知乙方後，終止本契約全部或部分標的之執行範圍，費用則依原約定價格按乙方實際執行比例減少。終止前尚未完成之工作，乙方應繼續執行至完成工作為止，且不得另向甲方收費。
- 5、 本契約終止時，自終止之日起，雙方之權利義務即消滅。契約解除時，溯及契約生效日消滅。乙方並負擔相關之保密義務。

第十二條 資訊安全維護

- 1、 乙方同意並要求其參與人員共同遵循資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守甲方訂定之「供應商管理作業標準」及甲方提供之相關作業規定。
- 2、 乙方應對系統開發之資安需求（機密性、完整性、可用性）進行確認。
- 3、 乙方之參與人員均應受過適當之資通安全教育訓練。甲方認有必要時，得要求乙方派員參與甲方所舉辦之相關課程。
- 4、 乙方執行本契約工作時，如違反資通安全相關法令或知悉發生資安事件時，必須立即通報甲方，提出緊急應變處置，並配合甲方做後續處理。
- 5、 乙方因執行本契約非經甲方同意，不得將資訊系統資料複製攜離甲方儲存位置，資訊系統資料處理必須在甲方指定地點為之。
- 6、 乙方因執行本契約，須存取甲方之資訊設施，須經甲方同意，始得為之。
- 7、 乙方存取本院之資訊設施時不得另行私接無線或行動網路通訊跨接甲方網路環境。
- 8、 乙方因執行本契約，須攜帶資訊設施連線甲方網路，須經甲方同意，始得為之。
- 9、 乙方因執行本契約交付之軟硬體及文件，應先行檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel），及弱點掃描等檢測證明。
- 10、 乙方因執行本契約工作而持有機關指定履約終止或解除後，乙方應返還、移交、刪除或銷毀履行本契約而持有之資料或依機關之指示返還或移交之資

料。但契約標的經納入變方其他契約維護或保園之範圍者，不在此限。

第十三條 稽核權

甲方得就下列事項進行不定期稽核，惟應於稽核日之五日前通知乙方，乙方應配合甲方辦理相關稽核事宜：

- 1、 本契約保密責任及資通安全條款等之執行情形。
- 2、 甲方於規範書中因考量受託者之專業能力與經驗、委外項目之性質及資通安全需求等因素，針對乙方及其參與人員之範圍與對象等，所訂之資格條件。
- 3、 甲方係因知悉乙方發生可能影響受託業務之資通安全事件，以稽核或其他適當方式確認受託業務之執行情形時，不受前項五日前通知之限制。
- 4、 核結果不符合前項應遵循規定或本契約之約定者，乙方於接獲甲方通知後應於期限內完成改善。

第十三條 個人資料保護

乙方因執行本契約需要，而蒐集、處理或利用第三人個人資料時，應符合個人資料保護法及其他相關法令規範，若有違反，致第三人個人資料遭不法蒐集、處理、利用或其他侵害情事者，應對該第三人負損害賠償責任，及承擔相關民、刑事及行政責任；如致甲方遭受損害或遭第三人提起訴訟時，亦應對甲方負損害賠償責任及因涉訟所應支付之費用，包含但不限於訴訟費用、律師費用及對第三人之賠償。

第十四條 人員管理

- 1、 乙方應自行約束其受雇人、受聘人、代理人或履行輔助人履約時之紀律、行為、操守。
- 2、 乙方若有為履行本契約而將其受雇人、受聘人、代理人或履行輔助人派至甲

方之情形時，乙方應對前述人員盡管理之責，並承擔前述人員因違反法令或不當行為致生之損害賠償責任。

第十五條 權利保留

任一方因權宜措施而未行使本契約權利，不得認為放棄權利、或免除他方義務、或影響其他權利之行使。

第十六條 契約生效與修改

本契約於雙方簽訂後自本契約第二條履約期間之始日起生效，取代契約簽定前雙方所有以口頭或書面之建議、協議或會談。本契約及其附件任何修改，應以書面為之。

第十七條 爭議處理

- 1、 履約爭議發生後，與爭議無關或不受影響之部分乙方應繼續履約，但經甲方同意者不在此限。
- 2、 本契約以中華民國法律為準據法。雙方因本契約所引起之爭議，應先自行協商解決，若仍須涉訟，雙方同意以臺灣臺北地方法院為第一審管轄法院。

第十八條 其他

- 1、 本契約第六條、第七條、第九條~第十七條、第十八條第一項約定，除本契約另有約定外，不因本契約之消滅而受影響。
- 2、 本契約正本壹式貳份，甲、乙以雙方各執壹份為憑。印花稅由雙方各自貼足。

立契約人：

甲 方：財團法人台灣設計研究院

代表人：張基義

地 址：臺北市信義區光復南路 1 3 3 號

統 編：99330539

電 話：02-27458199

契約編號：

乙 方：

代表人：

地 址：

統 編：

電 話：

中華民國 000 年 00 月 00 日

「設計導向 AI 知識基礎建置及驗證」採購案需求說明書 (含驗收規範)

1、案名：「設計導向 AI 知識基礎建置及驗證」採購案

2、購案期程與預算期程

(1) 期程：000 年 00 月 00 日起至 115 年 12 月 15 日止。

(2) 本案總預算為新臺幣 xxx 元整 (含稅)。

1、需求說明

(1) 系統標的

項目	功能說明	數量	備註
資安(普級) 優化與 系統維運	事件日誌與可歸責性 定期審查日誌 系統時鐘校準 日誌保護	1 式	
	營運持續計畫 定期測試備份資料 訂定系統中斷至恢復時間 系統中斷時，提供其他取代之方式	1 式	
	系統與服務獲得 識別威脅，進行風險分析與評估 風險評估結果進行安全修正 系統進行版本控制 區分開發、測試、正式環境	1 式	

	系統與資訊完整性 定期確認資通系統相關漏洞修補 資通系統監控攻擊事件 使用完整性驗證工具 使用者輸入合法性檢查置放於伺服器端 發現違反完整性時的安全保護措施	1 式	
--	---	-----	--

2、產品支援需求

- (1) 廠商所交之採購標的應自本案驗收合格之日起提供電話諮詢與技術支援服務，基本時間為星期一至星期五（不含國定假日）上午九點至下午六點，另行約定時間或例假日不在此限。
- (2) 技術支援方式：軟體發生任何問題，得標廠商須於接獲通知 2 個工作小時內開始協助解決，4 個工作小時內進行維修，並應於 8 個工作小時內恢復正常作業。

3、其他注意事項

聯絡人資料：

姓 名：曾唯哲

電 話：02-27458199 Ext. 287

E-Mail：weizhe_tzeng@tdri.org.tw

附件二

資通系統防護需求分級評估表

「設計導向 AI 知識基礎建置及驗證」安全等級評估表

功能說明：。

業務屬性：☐行政類 ☒業務類 日期：115 年 月 日

影響構面				資通系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	
普	普	普	普	普
系統最大可容忍中斷時間(小時)：				24
步驟 1：設定影響構面等級				
影響構面		安全等級	原因說明	
1.機密性	初估	普	系統資料不屬機敏性資料，當未經授權進行存取控制，造成資料外洩，對業務推行產生嚴重之影響。(參考文字)	
	異動			
2.完整性	初估	普	系統每日進行備份，當發生系統資料庫遭受未經授權者篡改，可進行備份還原作業，對業務推行產生有限之影響。(參考文字)	
	異動			

3.可用性	初估	普	系統中斷（例如：系統損毀、網路中斷），對業務推行產生有限之影響。（參考文字）
	異動		
4.法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果。（參考文字）
	異動		
步驟 2：識別業務屬性			
項目		業務屬性	原因說明
識別業務屬性	初估	業務類	
	異動		
備註			

附件三

設計導向 AI 知識基礎建置及驗證資通系統管理暨自我檢核表

☐ 本系統(網站)尚未建置系統(網站)，預計 年 月 日上線。 ☒ 本系統(網站)為後續維護之系統(網站)。						
一、資通系統防護基準自評表						
檢查項目					計畫執行單位自行查驗 (請計畫執行單位填寫說明，並勾選是否符合)	
主項目	次項目	系統防護需求	普	中	高	說明現有控制措施 符合性評估 (每題皆須勾選)
1.存取控制	1.1 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。 (應說明不使用身分證字號為帳號名稱)	★	★	★	☒ 符合 ☐ 不符合
	1.2 帳號管理	已逾期之臨時或緊急帳號應刪除或禁用。		★	★	☐ 符合 ☐ 不符合 ☒ 不適用
	1.3 帳號管理	資通系統閒置帳號應禁用。		★	★	☐ 符合 ☐ 不符合 ☒ 不適用

	1.4 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。(應說明週期，並以不超過半年為宜，須檢附審查紀錄)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	1.5 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	1.6 帳號管理	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。(說明系統登出時間)			★		☐ 符合 ☐ 不符合 ☒ 不適用
	1.7 帳號管理	應依機關規定之情況及條件，使用資通系統。(說明機關規定，包含組態)			★		☐ 符合 ☐ 不符合 ☒ 不適用
	1.8 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。(應設定特殊權限的嚴格管理措施)			★		☐ 符合 ☐ 不符合 ☒ 不適用

	1.9 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。 (範圍:運行於作業系統上之網站及資料庫相關應用程式[非使用作業系統最高權限帳號啟動])		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	1.10 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。	★	★	★		☒ 符合 ☐ 不符合
	1.11 遠端存取	使用者之權限檢查作業應於伺服器端完成。	★	★	★		☒ 符合 ☐ 不符合
	1.12 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。	★	★	★		☒ 符合 ☐ 不符合
	1.13 遠端存取	應採用加密機制。	★	★	★		☒ 符合 ☐ 不符合

	1.14 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
2.事件日誌與可歸責性	2.1 記錄事件	訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。(應保留以下 4 種 Log) 1.作業系統日誌(OS event log) 2.網站日誌(Web log) 3.應用程式日誌(AP log) 4.登入日誌(Logon log)	★	★	★		☒ 符合 ☐ 不符合
	2.2 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。(如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及等)	★	★	★		☒ 符合 ☐ 不符合
	2.3 記錄事件	應記錄資通系統管理者帳號所執行之各項功能。(如：帳號登出入、密碼變更、存取權限異動等)	★	★	★		☒ 符合 ☐ 不符合

	2.4 記錄事件	應定期審查機關所保留資通系統產生之日誌。(應說明週期，並以不超過每週為宜。)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	2.5 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。	★	★	★		☒ 符合 ☐ 不符合
	2.6 日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。(應配置最少 6 個月之儲存容量)	★	★	★		☒ 符合 ☐ 不符合
	2.7 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。(如：儲存容量空間不足，選擇進行封存，不要覆寫日誌資料)	★	★	★		☒ 符合 ☐ 不符合

2.8 日誌處理失效之回應	機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 (特定人員:系統相關人員)			★		☐ 符合 ☐ 不符合 ☒ 不適用
2.9 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)。	★	★	★		☒ 符合 ☐ 不符合
2.10 時戳及校時	系統內部時鐘應定期與基準時間源進行同步。(應說明週期，並以不超過每週為宜。)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
2.11 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。	★	★	★		☒ 符合 ☐ 不符合
2.12 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
2.13 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。 (應說明週期，並以不超過每週為宜。)			★		☐ 符合 ☐ 不符合 ☒ 不適用

3.營運持續計畫	3.1 系統備份	訂定系統可容忍資料損失之時間要求。	★	★	★		☒ 符合 ☐ 不符合
	3.2 系統備份	執行系統源碼與資料備份。	★	★	★		☒ 符合 ☐ 不符合
	3.3 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。(應說明週期，並以不超過每季為宜。)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	3.4 系統備份	應將備份還原，作為營運持續計畫測試之一部分。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	3.5 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	3.6 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。(須與當年核定之最大可容忍中斷時間相同)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用

	3.7 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
4.識別與鑑別	4.1 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。	★	★	★		☒ 符合 ☐ 不符合
	4.2 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	4.3 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。 (建議透過系統機制要求使用者登入後立即變更密碼)	★	★	★		☒ 符合 ☐ 不符合
	4.4 身分驗證管理	身分驗證相關資訊不以明文傳輸。	★	★	★		☒ 符合 ☐ 不符合
	4.5 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。	★	★	★		☒ 符合 ☐ 不符合

	4.6 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。 (密碼不少於 12 碼，且由大小寫、數字及符號組成混合，且需在一定期間[1~90 天]內變更)	★	★	★		■符合 □不符合
	4.7 身分驗證管理	密碼變更時，至少不可以與前三次使用過之密碼相同。	★	★	★		■符合 □不符合
	4.8 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。	★	★	★		■符合 □不符合
	4.9 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。 (應有 captcha 機制，請提供佐證)		★	★		□符合 □不符合 ■不適用
	4.10 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性符記。		★	★		□符合 □不符合 ■不適用

	4.11 鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。 (如:以*取代真實輸入字元)	★	★	★		☒ 符合 ☐ 不符合
	4.12 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	4.13 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)。	★	★	★		☒ 符合 ☐ 不符合
5.系統與服務獲得	5.1 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。	★	★	★		☒ 符合 ☐ 不符合
	5.2 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	5.3 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用

	5.4 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。 (系統發展生命週期皆適用) (14 為第 5 級之要求) (控制措施: 資安防護強度等級是否達第 4 等級(含)以上(詳附錄 40) ? 主機使用之防毒軟體及版本。 定期更新主機 patch。 (應說明週期，並以不超過每月為宜。) 網路具有防火牆防護。 網路或主機具有入侵偵測機制(IDS)。 網路或主機是否具有入侵防禦機制(IPS)。 網站是否設有反弱點防護機制(網站漏洞修補前之替代性防護機制) ? 資安防護設備(如防火牆、入侵防禦機制等)是否設有偵測與告警機制，並有專人定期檢視？	★	★	★		(1~13 項控制措施皆須符合才可勾符合) ■符合 □不符合
--	------------------	--	---	---	---	--	--

		(應說明週期，並以 不超過每週為宜。) 存放資通訊設備區域是否設有安全保護措施(例如門禁管理、不斷電(UPS)系統、空調設備、消防設備等)？ 機房各項安全措施是否定期檢查？ (應說明週期，並以 不超過每週為宜。) 電源供應是否有保護措施？(註：例如防雷擊、防突波、具發電機等。) 設備是否定期維護？ (應說明週期，並以 不超過每月為宜。) 對具儲存資訊之設備外送維修時，是否具有安全評估措施？(例：備份資料後，將外送設備的資料抹除後再送修。) 是否具有資訊安全防护中心 (SOC) 24 小時網路監控及通報機制？ 機房是否有 24 小時操作人員輪值？				
--	--	--	--	--	--	--

5.5 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。	★	★	★		☒ 符合 ☐ 不符合
5.6 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。	★	★	★		☒ 符合 ☐ 不符合
5.7 系統發展生命週期開發階段	執行「源碼掃描」安全檢測。			★		☐ 符合 ☐ 不符合 ☒ 不適用
5.8 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
5.9 系統發展生命週期測試階段	執行「弱點掃描」安全檢測。 (1.系統發展生命週期皆適用。 2.範圍為網頁、主機、網路系統且需涵蓋 OWASP 最新 TOP 10 中指出的網頁應用程式常見弱點的檢測。 3.修補掃描結果各等級之弱點，並應再次確認已無弱點。)	★	★	★		☒ 符合 ☐ 不符合

5.10 系統發展生命週期測試階段	執行「滲透測試」安全檢測。			★		☐ 符合 ☐ 不符合 ☒ 不適用
5.11 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。	★	★	★		☒ 符合 ☐ 不符合
5.12 系統發展生命週期部署與維運階段	資通系統不使用預設密碼。	★	★	★		☒ 符合 ☐ 不符合
5.13 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)			★	★	☐ 符合 ☐ 不符合 ☒ 不適用
5.14 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。	★	★	★		☒ 符合 ☐ 不符合

	5.15 獲得程序	開發、測試及正式作業環境應為區隔。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	5.16 系統文件	應儲存與管理系統發展生命週期之相關文件。(應以書面或電子化形式保存，並被納入管理程序)	★	★	★		☒ 符合 ☐ 不符合
6.系統與通訊保護	6.1 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	6.2 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	6.3 傳輸之機密性與完整性	支援演算法最大長度金鑰。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	6.4 傳輸之機密性與完整性	加密金鑰或憑證應定期更換。(應說明檢查週期，並以不超過每季為宜。)			★		☐ 符合 ☐ 不符合 ☒ 不適用

	6.5 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	6.6 資料儲存之安全	資通系統重要組態設定檔案及其他相關具保護需求之資訊應加密或以其他適當方式儲存。			★		☐ 符合 ☐ 不符合 ☒ 不適用
7.系統與資訊完整性	7.1 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。(應說明週期，並以不超過每月為宜，須檢附測試佐證)	★	★	★		☒ 符合 ☐ 不符合
	7.2 漏洞修復	定期確認資通系統相關漏洞修復之狀態。(應說明週期，並以不超過每週為宜。)		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	7.3 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。(特定人員:系統相關人員)	★	★	★		☒ 符合 ☐ 不符合
	7.4 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用

	7.5 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。			★		☐ 符合 ☐ 不符合 ☒ 不適用
	7.6 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	7.7 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	7.8 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。		★	★		☐ 符合 ☐ 不符合 ☒ 不適用
	7.9 軟體及資訊完整性	應定期執行軟體與資訊完整性檢查。 (應說明週期，並以不超過每季為宜。)			★		☐ 符合 ☐ 不符合 ☒ 不適用

單位名稱：

單位負責人或代表人：

地址：

統一編號：

附件四

本案參與人員組織表

姓名	職稱	聯絡方式	工作內容
			1.

附件五

資料返還切結書

OO 公司 已確認自民國(以下同)11x 年 月 日起至民國 11x 年 月 日止，承接貴院「設計導向 AI 知識基礎建置及驗證」案（以下簡稱「本服務」），本案結束後相關業務資料及因本案蒐集之參與人員以外個人資料已協助：

☐ 返還貴院

☐ 銷毀

☐ 沿用保留至「 」

茲以本切結書為證。

此致 財團法人台灣設計研究院

法人名稱：

負責人：

地 址：

統一編號：

中華民國 11x 年 月 日

附件六

資訊安全暨個資保密同意書

茲緣於簽署人 (簽署人姓名，以下稱簽署人) 參與.....公司 (以下稱乙方) 受財團法人台灣設計研究院 (以下稱甲方) 委託執行「設計導向 AI 知識基礎建置及驗證案」(以下稱「本案」)，於本案執行期間有知悉或可得知悉或持有甲方機密資訊，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第1條、 簽署人承諾於本同意書有效期間內及本同意書期滿或終止後，對於所得知或持有一切甲方未標示得對外公開之公務秘密，以及甲方依同意書或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本同意書目的範圍內，於甲方指定之處所內使用之。非經甲方事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至甲方或甲方所指定處所以外之處所。

第2條、 簽署人知悉或取得甲方機密資訊應限於其執行本案所必需且僅限於本同意書有效期間內。簽署人同意該機密資訊，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第3條、 簽署人在下述情況下解除其所應負之保密義務：

1. 原負保密義務之資訊，由甲方提供以前，已合法持有或已知且無保密必要者。
2. 原負保密義務之資訊，依法令業已解密、依同意書甲方業已不負保密責任、或已為公眾所知之資訊。
3. 原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第4條、 簽署人若違反本同意書之規定，甲方得請求簽署人及其任職之乙方賠償甲方因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之乙方亦應負賠償責任。

第5條、 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第6條、 本同意書甲方執正本一份，簽署人及乙方執存影本一份。

第7條、 鑑於乙方提供之系統平台涉及蒐集、處理或儲存個人資料，簽署人及其所屬之乙方應配合甲方之資通安全與個資保護政策，於本案執行期間配合填覆並提交以下文件，作為資訊安全與委外風險控管之依據：

1. 委外廠商資訊安全管理自評表

2. 安全等級評估表

3. 資通系統防護基準自評表

簽署人姓名：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中華民國 11x 年 月 日

附件七

案名：設計導向 AI 知識基礎建置及驗證案 服務水準協議 (SLA)

一、目的

本服務水準協議 (SLA) 旨在訂定 Web-App 系統服務之可用性、回應時間、維運支援等服務指標，以確保系統穩定運作，保障使用者權益。

二、服務範圍

本協議適用於下列服務項目：

1. 報名系統前后台 (含使用者報名、管理者審查)
2. 資料庫儲存與備援服務
3. 驗證寄信、報名通知等系統通知服務
4. 系統帳號管理與權限控管
5. 維運監控與事件通報服務

三、服務可用性

服務項目	可用時間	年可用率	備註
------	------	------	----

契約編號：

案名：xxxxxx	12 小時 / 每日	≥ 95.5%	每年容許不可用時間約 24 小時內
-----------	------------	---------	-------------------

四、維運回應時間

事件等級	事件說明	回應時間	處理時間	備註
P1 - 嚴重	系統全面無法使用、資料遺失、無法登入	30 分鐘內	1 小時內恢復或提供暫時替代方案	365 天全年無休支援
P2 - 中度	單一功能異常、不影響整體服務	1 小時內	1 個工作日內修復	工作日支援
P3 - 一般	介面顯示錯誤、內容調整、使用者操作問題	1 小時內	1 個工作日內處理	工作日支援

五、維運支援窗口

支援時間：週一至週五 09:00–18:00 (不含國定假日)

通報方式：

契約編號：

- Email：xxx@xxx.com

- 緊急聯絡電話：xxxxxxx

通報內容須包含：問題描述、發生時間、操作步驟、影響範圍、螢幕截圖（如有）

六、資料備份與還原

- 備份頻率：每月自動備份
- 保留期限：最近 3 個月資料
- 還原服務：於接獲書面申請後 1 個工作日內完成指定日期資料之還原

七、安全性與合規

- 本系統符合資安法及個人資料保護法相關規定
- 傳輸資料均採用 HTTPS 加密通訊協定
- 管理者登入採取多重身分驗證（MFA）機制
- 每半年執行一次弱點掃描與系統安全性檢查

八、違約處理

若年度可用率低於 95.5%，可依據合約條款申請服務抵扣或金額賠償。

九、修訂與例外

本 SLA 如需變更，將提前通知使用單位，雙方協議後方可生效。因不可抗力

(如自然災害、國際資安攻擊) 導致之服務中斷不納入違約計算範圍。

契約編號：

附件八

報價單