交通部觀光署廠商資通安全管理約定書

(113.8.2 修定)

廠商承攬本採購案，若有涉及資通系統/網站、資通訊軟硬體建置、維運及資通服務提供等作業，須確實遵守下列規定：

一、建置及維運

(一) 新建置外部服務系統至少前台須採響應式(RWD)網頁設計技術製作，可配合不同行動裝置畫面大小變換頁面尺寸，但不得有照片變形情形出現；若因特殊需求無法採響應式(RWD)網頁設計，可敘明理由並經本署同意後不施作。

(二) 新建置外部服務系統需符合數位發展部各項網頁建置規範，包括「網站無障礙規範」、「政府網站服務管理規範」等，及通過無障礙網頁 AA 級檢測並取得標章；若因特殊需求無法取得無障礙網頁 AA 級檢測標章，可敘明理由並經本署同意後不施作。

(三) 若系統已採響應式(RWD)網頁設計或取得無障礙網頁 AA 級檢測標章，廠商須持續維持相關功能及作業。

(四) 外部服務系統網頁遭置換或發生異常，應於 10 分鐘內切換為備用之靜態服務畫面，並檢測修補弱點及備妥後續因應作法。

(五) 系統前後台應採用 https 加密方式，其協議應符合安全的國際傳輸標準，以維護資料傳輸安全及確保安全控管。

(六) 廠商應定期檢視網頁內圖文資訊及連結設定之正確性，並修正相關問題。

(七) 系統若未使用本署網域，應將網域租賃相關資訊(包含網址申請公司資訊、申請人資訊、申請帳號及密碼、租賃到期時間等)交付本署；契約及保固期間之網域租賃費用由廠商支付。

(八) 系統上線前或功能擴充/改版完成後，廠商應提出網頁應用程式之弱點掃描及程式原始碼安全檢測報告、壓力測試報告，另需配合本署資安檢測作業修正相關弱點。

(九) 本署或廠商所提出之各式資安檢測結果，嚴重、高、中及 OWASP TOP 10 以上之風險弱點，廠商須於 10 日內完成修補；低風險弱點，廠商須於契約期間內儘力完成修補；未能修補之風險，須於報告書或填寫「弱點處理報告單」，敘明無法修補原因、因應方法或相關資安防護作為，經本署審查同意後，始能延後修補時間。

(十) **本系統防護需求等級為：___級**(未載明者為中級)，履約期間廠商須填寫「資通系統防護基準表」(系統含有個人資料者須另外填寫「委外廠商自我評估表」)並送交本署審查，本署可視需求至廠商網頁或系統開發處所進行查核確認。廠商須依本署判定之系統防護需求等級(普、中、高)，完成「資通安全責任等級分級辦法」附表十資通系統防護基準規定之控制措施。

二、 環境及服務

(一) 本署可提供本案作業系統(Windows Server 2019)、資料庫(SQL Server 2019 或 2022)之虛擬主機環境，供得標廠商使用(若廠商需使用其他作業系統及資料庫需自行提供及安裝有版權之軟體，安裝之軟體需為最新版本，並需定期更新)。廠商可自行提供雲端環境放置本案系統，但須於專案及保固期間提供充足之對外網路及軟硬體資源，並提供防毒軟體、防火牆(WAF)、IPS、防止 DDoS 攻擊服務等基本資安防護，及提供系統與資料備份服務，相關費用由廠商支付。

(二) 如需申請本署共構機房虛擬主機環境或網域應填寫「資訊服務申請單」，經本署承辦單位主管核可後，向本署資訊管理單位提出申請。

(三) 軟硬體設備、網路環境及系統需符合 IPv6 規範(支援 IPv6 協定)及提供 IPv6 服務。

(四) 系統若放置於本署共構機房，廠商應配合本署資通安全要求辦理，如安裝代理程式執行安全監控等，及配合本署作業系統及資料庫升級、軟硬體設備汰換更新、虛擬環境調整等，完成相關搬移及設定等作業。

(五) 如需申請本署共構機房虛擬主機環境或網域，以及網頁或網址若有異動(包含新增或下架或修改名稱及網址)，應填寫「資訊服務申請單」，經本署承辦單位主管核可後，向本署資訊管理單位提出申請。

(六) 本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，且不得提供及使用大陸廠牌資通訊產品(包含系統軟體、APP、IoT 設備、行動裝置及手機、電腦、伺服器、監視器、遙控無人機、具資料處理或控制功能之硬體)。

(七) 本採購若屬經濟部投資審議司公告「具敏感性或國安(含資安)疑慮之業務範疇」之資訊服務採購，廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議司公告之陸資資訊服務業者。(上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議司網站)。

(八) 契約期間，廠商應負本案提供之系統及設備維護之責，使其能經常保持良好而可用狀況，若故障時，應於 2 小時內到場服務或著手處理，並於同一電話、電子郵件或簡訊等通知後 **小時內**(未載明者為 8 小時)維修完畢。若有正當理由無法於時限內到場提供服務或維修完畢，廠商應提供同級(含)以上備品替用，至故障設備或系統修復至正常運作。

三、 系統設計安全

(一) 系統設計若涉及身分驗證機制時，可優先考慮與其他安全驗證機制整合，並以較嚴謹之機制為優先，例如授權認證(CA)機制、輕量級目錄存取協定(LDAP)、作業系統帳號整合(如 SSO 或 AD)等。

(二) 採用帳號與密碼之身分認證機制時，密碼應考慮包含密碼長度限制、密碼組合限制、密碼錯誤次數限制與變更密碼歷史管理等，並符合政府組態基

準(Government Configuration Baseline, GCB)相關項目規定；若因特殊需求無法符合 GCB 規定，可敘明理由並經本署同意後不施作。

(三) 系統資訊若涉及機敏性資訊的傳輸與接收，應設計加密傳輸機制，並記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗等資訊;機敏性資料應加密處理,資料庫之程式應有過濾 SQL Injection 機制。

(四) 須留存系統至少最近 6 個月相關電磁紀錄，包含作業系統日誌(OS event)、網站日誌(web log)、應用程式日誌(AP log)及登入日誌(logon log)紀錄。

(五) 設計各種例外狀況處理機制時，應避免直接顯示原始完整錯誤資訊給予使用者。

(六) 程式失敗時，可能產生的錯誤碼應交由例外程式處理(Exception handling)。

(七) 系統建置應規劃適當之閒置時間，於使用者登入超過 30 分鐘且無任何動作時，應自動將其帳號登出。

(八) 系統應用程式編碼時，應避免撰寫不當造成跨網站的指令碼(Cross Site Scripting)、注入缺失(Injection Flaw)、惡意檔案執行(Malicious File Execution)、不安全的物件參考(Insecure Direct Object Reference)及跨網站的偽造要求(Cross-Site Request Forgery)等不安全源碼問題，並於網頁正式上線前於網頁應用程式之弱點掃描及程式原始碼安全檢測報告中說明。

(九) 廠商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)，提出安全性檢測證明，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

(十) 系統開發作業環境需有安全保護措施，開發測試及正式運作環境需予以區隔，並不得於系統正式作業環境進行資料測試；若因業務需要需以真實資料在測試系統進行資料測試，應取得本署授權後始能進行，且敏感資料或欄位應予以虛擬或模糊化。

(十一)廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

(十二)系統開發完成上線後，應提供一份可執行之完整版本程式及程式原始碼由業務負責人負責管理與控管，後續相關之異動管理應提交相關程式版本及程式原始碼作為備份或因應緊急復原時使用；若因特殊原因無法提供，可敘明理由並經本署同意後不提供。

(十三)廠商執行系統維護作業，如版本更新、異動資料檔或變更設定等，應提出需求變更並填寫「程式需求申請單」,經系統管理人員或業務權責單位審核後始得進行變更事宜，相關紀錄應留存備查。

(十四)廠商應配合本署資通安全要求，定期進行備份資料回復測試及業務永續計畫復原演練，並針對委外標的建立緊急應變計畫。

(十五)廠商對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人

員使用，並僅授權本署人員與廠商因職務所需之必要存取權限，且定期審查存取權限是否適當。

(十六)廠商人員如因作業需求，需對本署系統進行遠端存取，應填寫「網路服務連線申請單」提出申請，經本署權責單位主管核可後，方可開啟遠端服務。

(十七)廠商於履行契約期間所使用之軟體，須為合法，並不得違反智慧財產權之規定，如有違法情事發生，廠商須承擔應負之法律責任。

(十八)廠商所使用之工具軟體及處理作業之執行紀錄，本署有權進行稽核審查，廠商須配合提供相關資訊。

四、 資料庫使用安全

(一) 重要系統服務應考量有專屬資料庫，並應有防止使用者直接存取資料庫之設計，資料庫之異動應填寫「資訊服務申請單」提出申請，經本署承辦單位主管核可後，方可實施。

(二) 資料庫建置後，應立即更改所有管理權限之使用者密碼，防止非法連接資料庫；另資料庫管理系統在不影響系統效能下評估啟動稽核功能、保存資料庫管理系統特殊權限之異動記錄、使用者帳號新增、刪除等異動記錄、物件之建立、修改及刪除等紀錄至少保留 6 個月。

五、 資訊服務安全

(一) 辦理本署資通系統建置、維運或資通服務提供、代表本署處理資料之委外及複委託(分包、轉包…等)廠商應遵守本署契約及相關安全要求，及具備資通安全維護措施，惟未經本署許可，不得將資料處理再行分包委外。

(二) 接觸本署資料之廠商服務人員應依據本署資通安全管理制度要求簽署「保密切結書(廠商、人員)」，專案執行期間，廠商人員若有異動應比照辦理補足相關資料。

(三) 履約完成或契約終止或解除時，廠商須交付最後 1 版可執行之完整版本程式及程式原始碼、系統資料庫等，及契約期間所蒐集之資料(含民眾參與活動投稿原始資料、民眾個人資料等)，若網頁或系統經本署評估已無存在需求，則需協助進行下架及資料刪除作業，廠商並需將執行本案契約業務而蒐集、處理、利用之個人資料予以刪除，且不得留存任何備份。

(四) 廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合本署對系統品質及資通安全的要求。

(五) 廠商於知悉本案違反資通安全相關法令或系統發生資通安全事件時，應立即向本署之權責人員或窗口，以指定之方式進行通報，並提出緊急應變處置，及採行補救措施，並配合本署做後續處理。

(六) 廠商辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

(七) 廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似

業務經驗之資通安全專業人員。

(八) 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(九) 受託業務包括客製化資通系統開發者，廠商應提供系統之安全性檢測證明；系統屬本署之核心資通系統，或委託金額達新臺幣一千萬元以上者，廠商應委託第三方進行安全性檢測(相關費用由廠商支付)。

(十) 廠商利用非自行開發之系統或資源者(例：外部元件或軟體)，應提供清單，並標示非自行開發之內容、版本、來源及提供授權證明，並注意其安全漏洞通告，且定期評估更新。

(十一) 契約履約或解除時或終止後，廠商應返還、移交、刪除或銷毀執行服務所持有之相關資料，或依本署之指示返還之，並保留執行紀錄。

(十二) 本署應定期或於知悉廠商發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

(十三) 廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本署資通安全管理及保密相關規定。此外本署保有對廠商及其分包廠商以派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他適當方式執行相關稽核或查核的權利，稽核結果不符合本案契約約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本署通知後應於期限內完成改善。

(十四) 廠商保證對於其受雇人或受聘人職務上完成之著作，依著作權法第 11 條第 1 項但書及第 12 條規定，與其受雇人或受聘人約定以廠商為著作人，享有著作人格權及著作財產權(須提交著作人約定書)。惟此一約定僅止於廠商與其受雇人或受聘人間。廠商與機關間之權利及責任，仍以本案契約為準。

六、個人資料保護

(一) 若本署委託處理之資料涉及個人資訊時，廠商或分包商皆應嚴守「個人資料保護法」及「個人資料保護法施行細則」相關要求，做到資料之處理與利用為適當、相關且不過度。另應載明個人資料保密聲明及依個資法及相關法令應受監督之事項，並提出適當之『檔案安全維護計畫』及『業務終止後個人資料處理辦法』。

(二) 廠商依本案受本署委託蒐集、處理或利用個人資料及檔案（即個人資料保護法所指自然人之姓名、身分證統一編號、職業、聯絡方式、社會活動、其他得以直接或間接方式識別該個人之資料）時，廠商應遵守下列約定：

1. 蒐集、處理或利用時之義務

(1) 廠商基於本案蒐集、處理或利用個人資料時，應符合個人資料保護法第 19 條或第 20 條要件及個人資料保護法施行細則等相關規定，及符合本署所委託之範圍、類別、特定目的及期間。

(2) 廠商僅得於本案執行範圍內，蒐集、處理或利用個人資料（廠商不得

利用本署所提供或因執行本案所蒐集之個人資料及檔案進行行銷或商業推銷等相關活動，或以任何方式或方法交付予履約無關之第三人，亦不得為本案計畫工作以外之蒐集、處理或利用，含結合廠商原自己所保有之個人資料及檔案，再為處理或利用）。

(3)廠商認為本署指示有違反個人資料保護法或其他法令者，應立即通知本署，並經同意後停止執行該作業事項。

2.安全管理措施

廠商在執行業務所必須之範圍內，應依個人資料保護法第 27 條規定採行個人資料保護法施行細則第 12 條所規定之安全管理措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。安全管理措施得包含下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

(1) 配置管理之人員及相當資源。

(2) 界定個人資料之範圍。

(3) 個人資料之風險評估及管理機制。

(4) 事故之預防、通報及應變機制。

(5) 個人資料蒐集、處理及利用之內部管理程序。

(6) 資料安全管理及人員管理。

(7) 認知宣導及教育訓練。

(8) 設備安全管理。

(9) 資料安全稽核機制。

(10) 使用紀錄、軌跡資料及證據保存。

(11)個人資料安全維護之整體持續改善。

3.廠商執行業務上若有複委託之需求，就涉及個人資料之蒐集、處理、利用之行為應事前取得本署之書面同意及該複委託廠商對於個人資料保密之書面承諾，並以書面通知本署複委託廠商之名稱、地址及個人資料之蒐集、處理、利用之範圍。廠商應限定複委託方蒐集、處理、利用個人資料之範圍，並對該複委託方依個人資料保護法等相關規定進行適當之監督。廠商對於複委託廠商蒐集、處理、利用個人資料之行為應負同一責任。

4.當事人權利行使時之義務

廠商執行本案業務，接獲個人資料當事人行使權利時，應依相關規定予以回覆，並做成紀錄，供本署備查。

5.資料提供義務

本署要求廠商提供所蒐集之個人資料檔案、個人資料檔案保有之依據及特定目的、個人資料之類別等相關資訊及其蒐集、處理、利用之相關資料時，廠商不得拒絕。

6.緊急事故通知義務

廠商因執行本案，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，

於發現後，應立即通知本署並採取因應措施；廠商於查明後應將其違反情形、涉及個資範圍、採行及預定採行之補救措施，經本署同意後，依法以適當方式通知當事人。

7. 定期確認

本署得針對廠商的個人資料安全管理措施實施情形進行稽核確認，並將確認結果記錄之；必要時，得派員進行實地訪查或委託專業人員進行稽核，廠商應予配合。本署於訪查或稽核後，認有缺失，得以書面敘明理由請廠商限期改善。

8. 履約中或契約終止時資料的刪除或返還

(1) 於履約中本署得隨時要求廠商及處理個人資料之相關人員將執行本案業務而蒐集、處理、利用之個人資料返還本署或予以刪除，且不得留存任何備份。

(2) 本案契約終止或解除時，廠商及處理個人資料之相關人員應刪除或銷燬履行契約而持有之個人資料，及返還個人資料之載體；並提供刪除、銷燬或返還個人資料之時間、方式、地點等紀錄。

(3) 前項返還，廠商得以交付本署指定之第三人為之。廠商刪除、銷燬作業，本署於必要時，得實地查訪，廠商應予配合。

9. 損害賠償責任

(1) 廠商違反本約定書第 6 點第 2 款第 1 目至第 8 目提出限期改善建議，廠商未依期限改善時，本署得依情節輕重為以下處理：

A. 以書面通知廠商終止或解除契約之部分或全部。

B. 要求減少部分或全部價金。

C. 按契約總價的千分之 2，計收違約金。

(2) 廠商因執行本案業務而違反個人資料保護法、個人資料保護法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。本署如因廠商執行本案而違反個人資料保護法、個人資料保護法施行細則，而遭受損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任(如於訴訟中，廠商應協助本署為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償本署因此對第三人所負之損害賠償責任)。

七、保密及著作權簽署

(一)廠商承攬本採購案，若有涉及資通系統/網站、資通訊軟硬體建置、維運及資通服務提供等作業，廠商或團隊成員須簽署及交付下列文件：

1. 保密同意書/保密切結書(廠商)1 份。

2. 保密同意書/保密切結書(人員)：參與本案相關人員各簽署 1 份。

3. 著作人約定書：參與本案相關人員各簽署 1 份。

4.廠商服務團隊成員名冊1份。

5.廠商人員接受適任性查核同意書：本委外案涉及重要業務及國家機密者，參與本案相關人員各簽署1份。

(二)若團隊成員有異動，新任人員應於到任當日或到任前，提交保密同意書/保密切結書(人員)、著作人約定書。

以上資安相關規定事項，本公司已確實明瞭，並允諾確實遵守，如有違反，願接受本案契約相關罰則之處分。

廠商名稱及蓋章：

廠商負責人姓名及簽章：

廠商地址：

廠商聯絡電話：

統一編號：

中　　華　　民　　國　　年　　月　　日

保密同意書/保密切結書(廠商)

公司（以下簡稱廠商）受交通部觀光署北海岸及觀音山國家風景區管理處（以下簡稱機關）委託辦理**114 年度觀音山遊客中心 D 棟出租案**（以下簡稱本案），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密(包含個人資料)，為保持其秘密性，同意恪遵本切結書下列各項規定：

第一條　廠商承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約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，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，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，亦不得攜至機關或機關所指定處所以外之處所。

第二條　廠商知悉或取得機關公務秘密、業務秘密及任何個人資料，應限於其執行本契約所必需且僅限於本契約有效期間內，提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條　廠商在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

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。

第四條　廠商違反本切結書之規定，致造成機關或第三者之損害或賠償，廠商同意無條件負擔全部責任，包括因此所致機關或第三人涉訟，所須支付之一切費用及賠償。於第三人對機關提出請求、訴訟，經機關以書面通知廠商提供相關資料，廠商應合作提供。

第五條　廠商對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料、個人資料等，均保證善盡保密義務與責任，並遵循「營業秘密法」、「著作權法」、「商標法」、「專利法」、「個人資料保護法」及「個人資料保護法施行細則」等相關規定，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，此外，廠商處理個人資料檔案部分應於委託關係解除或終止時刪除或銷燬履行契約而持有之個人資料，及返還個人資料之載體；並提供刪除、銷燬或返還個人資料之時間、方式、地點等紀錄，機關保有查核之權利。

1. 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。
2. 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機

或無線傳輸等網路設備連接外部網路。

3. 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
4. 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。
5. 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
6. 本切結書不因立切結書人離職而失效。
7. 立切結書人因違反本切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

第六條　廠商若違反本切結書之規定，機關得請求廠商賠償機關因此所受之損害及追究廠商洩密之刑責，如因而致第三人受有損害者，廠商亦應負賠償責任。

此致

交通部觀光署北海岸及觀音山國家風景區管理處

立切結書人

廠商名稱及蓋章：

廠商負責人姓名及簽章：

廠商地址：

廠商聯絡電話：

統一編號：

機關蒐集本表單上所列之個人資料，作為辨識您為簽署本切結書之本人，並為追溯違反本切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與機關個資保護之要求辦理。

中　　華　　民　　國　　年　　月　　日

保密同意書/保密切結書(人員)

公司（以下簡稱廠商）　　(公司人員，以下簡稱甲方)受交通部觀光署（以下簡稱機關）委託辦理**114年度觀音山遊客中心D棟出租案**（以下簡稱本案），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密(包含個人資料)，為保持其秘密性，同意恪遵本切結書下列各項規定：

第一條　甲方承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約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，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，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，亦不得攜至機關或機關所指定處所以外之處所。

第二條　甲方知悉或取得機關公務秘密、業務秘密及任何個人資料，應限於其執行本契約所必需且僅限於本契約有效期間內，提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條　甲方在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

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。

第四條　甲方違反本切結書之規定，致造成機關或第三者之損害或賠償，甲方同意無條件負擔全部責任，包括因此所致機關或第三人涉訟，所須支付之一切費用及賠償。於第三人對機關提出請求、訴訟，經機關以書面通知甲方提供相關資料，甲方應合作提供。

第五條　甲方對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料、個人資料等，均保證善盡保密義務與責任，並遵循「營業秘密法」、「著作權法」、「商標法」、「專利法」、「個人資料保護法」及「個人資料保護法施行細則」等相關規定，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，此外，甲方處理個人資料檔案部分應於委託關係解除或終止時刪除或銷燬履行契約而持有之個人資料，及返還個人資料之載體；並提供刪除、銷燬或返還個人資料之時間、方式、地點等紀錄，機關保有查核之權利。

1. 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。
2. 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資

訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

3. 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
4. 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。
5. 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
6. 本切結書不因立切結書人離職而失效。
7. 立切結書人因違反本切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

第六條　甲方若違反本切結書之規定，機關得請求甲方及其任職之廠商賠償機關因此所受之損害及追究廠商洩密之刑責，如因而致第三人受有損害者，甲方及其任職之廠商亦應負賠償責任。

此致

交通部觀光署北海岸及觀音山國家風景區管理處

立切結書人

姓　　名：_____

地　　址：_____

機關蒐集本表單上所列之個人資料，作為辨識您為簽署本切結書之本人，並為追溯違反本切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與機關個資保護之要求辦理。

中　　華　　民　　國　　年　　月　　日

著作人約定書

受雇(聘)人＿＿＿＿＿＿＿＿於雇(聘)用人＿○○○公司＿＿雇(聘)用期間內，在雇(聘)用人執行交通部觀光署**114年度觀音山遊客中心D棟出租案**契約由受雇(聘)人所完成之著作，茲約定均以雇(聘)用人為著作人，此證。

立約定書人　雇(聘)用人/廠商：

代表人：

地址：

立約定書人　受雇(聘)人：

身分證字號：

地址：

中　華　民　國　年　月　日

廠商服務團隊成員名冊

廠商及分包商名稱及地址	廠商及分包廠商國別	姓名	職稱	國籍	學歷/經歷	負責工作項目

廠商人員接受適任性查核同意書

本人於民國　　年　　月　　日至於民國　　年　　月　　日間，因任職----------（廠商名稱）受交通部觀光署北海岸及觀音山國家風景區管理處之委託，執行**114 年度觀音山遊客中心 D 棟出租案**(業務)，涉及該機關之重要業務及國家機密，依資通安全管理法第九條及資通安全管理法施行細則第四條之規定，同意交通部觀光署北海岸及觀音山國家風景區管理處以下列事項進行適任性查核：

1、是否曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

2、是否曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

3、是否曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

4、其他與國家機密保護相關之具體項目。

簽署人姓名及簽章：

身分證字號：

通訊地址：

聯絡電話：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中　　華　　民　　國　　年　　月　　日