# 產業園區安全防護系統環域分析功能優化採購規格

## 一、工作內容

(一) 建置鄰近工廠化學品風險圖台介面(1 工廠呈現畫面)

(二) 建置鄰近工廠化學品風險圖台介面(1 園區呈現畫面)

## 二、資安配合事項

(一) 程式碼有異動時，需檢附版本更新紀錄表。

## 三、期程：

(一) 保固期間：自系統功能完成後為期一年。

(二) 以上維護項目，若有移機或變更而致系統、設備停止使用情形，採購單位可視需要終止該項目之維護，維護費用則結算至該月月底為止。

(三) 維護時間：本合約之基本維護時間為除國定例假日或當地縣市政府因故宣佈為非上班之日(以行政院人事行政總處規定為準)以外之星期一至星期五自上午 8 時至下午 5 時 30 分止之時段。

(四) 若有緊急狀況，則維護時間可不受一般時間之限制。

## 四、維護範圍

(一) 採購單位擁有系統程式總量 15% (程式支次或網頁版頁次)之新增修改權利。

(二) 得標廠商必需概括承受本計畫相關原始程式設計錯誤所造成之使用障礙，需免費負責除錯，並於維護需求單要求期限內完成。唯採購單位必需提供所有相關之原始程式碼，以利任務之遂行。

(三) 得標廠商必需概括承受環境部、化學署及本單位年度內預計完成或臨時交辦之工作事項。

## 五、網站與資料庫服務維護要求

(一) 上班時間內(週一至週五上午八時至下午五時)提供電話或電子郵件諮詢。承包商進行網站例行性維護需事前提出申請，視情況遠端或派員至台北機房內維護。

(二) 上班時間外提供專人及專線電話緊急應變之用。

(三) 承包商必需同意於基本維護時間內接獲甲方修護通知起 4 小時內，派遣工程師到場服務或電話線上解答，並於 48 個工作小時內修復。

(四) 承包商必需協助建置備援網站服務(備援主機由採購方提供)，當發生緊急事故(如：電力中斷等)，使採購單位網站無法正常運作時，承包商需能確保備援網站服務正常。

(五) 重大狀況處理：承包商於維護期間內，如因維護標的物故障造成系統停止運作無法使用，承包商應於收到採購單位維護申請後，於 8 工作小時內排除故障使系統正常運作，並於故障排除後 7 日曆天內提出異常原因分析及復原方法之報告予收到採購單位。

(六) 不另外提供承包商到場服務差旅費。

## 六、 保密及資訊安全條款

如附件一。

## 七、 個人資料保護條款

如附件二。

## 八、違約罰則

(一) 除經採購單位同意外，若未於 4 個工作小時內回應甲方需求或 48 工作小時內未能修復，每逾工作一小時，則承包商同意按每月該項維護費用之千分之一金額扣罰給付採購單位，其中逾期部分計最高該項維護費百分之二十為限，惟若情形特殊經採購單位同意者以及新增功能之程式經雙方約定之工作時程等兩項範圍內不在此限。

(二) 承包商於上班時間外所以提供專人及專線電話，如於緊急應變時經採購單位使用未能暢通或無人接聽，經採購單位連續警告累積達三次，並經採購單位認定確為承包商疏失。則承包商同意每次按總維護金額百分之一金額扣罰給付採購單位，最高累計可達總維護金額百分之二十為限。

(三) 本計畫提供之相關資訊機密，係指使用電腦設備製作、保存與機密有關之資料，及處理該資料有關之系統、程式、消息或文件。由於事涉資料提供單位之隱私權，

除經採購單位同意外，承包商不得對外提供相關資訊，如若發現計畫提供之相關資訊機密由承包商外流或盜用並查證屬實，承包商除無異議賠償本公司懲罰性違約金外，其違法行為並應自負其法律責任。

## 九、付款方式

本維護計畫分二期支付，憑交付資料及發票依照本院行政手續請領費用。

(一) 第一期：於 115 年 06 月 30 日前完成工作內容(一)，憑出貨單及發票始撥付第一期款（請領契約價金總額百分之 60）。

(二) 第二期：於 115 年 10 月 30 日前完成其餘工作內容，憑出貨單及提交本單位整體網站及資料庫設計架構與對應資料、有關程式碼及安裝程式等始撥付尾款（請領契約價金總額百分之 40）。

## 附件一、保密及資訊安全條款

（一）本條款所稱保密之文件及資料，係指：

1. 在業務上認為不對外公開或定義為密、機密、極機密或絕對機密之一切文件及資料，包括與其業務或研究開發有關之內容。
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。
3. 與本案工作有關，其成果尚不足以對外公布之資料、訊息及文件。

（二）廠商承諾於本案有效期間內及本案期滿或終止後，對於所得知或持有一切未標示得對外公開之公務秘密，以及依契約或法令對第三人負有保密義務未標示得對外公開之業務私密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本案目的範圍內，於本院指定之處所內使用之。非經本院事前書面同意，廠商不得為逾越權限範圍之利用，或為本人或任何第三人之需要而複製、保有、利用該等機密或將之洩漏、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機密，或對外發表或出版，亦不得攜至本院或本院所指定處所以外之處所。

（三）廠商知悉或取得本院之公務秘密與業務秘密應限於其執行本案所必需且僅限於本案有效期間內利用。廠商同意本條款所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之廠商團隊成員，並應要求該等人員簽署與本條款款內容相同之保密同意書或保密切結書。(範本參見附件三或附件四)

（四）廠商在下述情況下解除其依本條款款所應負之保密義務：

1. 廠商原負保密義務之資訊，由本院提供以前，已為廠商所合法持有或已知且無保密必要者。
2. 廠商原負保密義務之資訊，依法令業已解密、依契約本院業已不負保密責任、或已為公眾所週知之資訊。
3. 廠商原負保密義務之資訊，係廠商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。

（五）廠商同意其人員、代理人、經本院同意複委託之受託人或使用人如有違反本條款或其自行簽署之保密同意書者，視同廠商違反本條款之保密義務。

（六）契約內容有須保密者，廠商未經本院書面同意，不得將契約內容洩漏予與履約無關之第三人。

（七）廠商履約期間所知悉之本院機密或任何不公開之文書、圖畫、消息、物品或其他資訊，均應保密，不得洩漏。

（八）廠商因履行本案而須將本案內容或因履行本案而取得之應保密文件及資料揭露予第三人時，應以該第三人與履約有關，且揭露之內容應為該第三人確有必要知悉者為限。

（九）廠商應使廠商執行本案之人員，包括但不限於經本院同意複委託之受託人、分包廠商等，以書面切結保密義務，並受本條款之拘束。

（十）廠商計畫主持人及參與計畫工作人員，均應嚴守委託契約執行內容及本院之業務機密，並不得有侵害及損及本院權利之行為。廠商應與其所聘用執行本計畫之研究人員訂定研究成果歸屬方式、保密條款及廠商之聘用研究人員違反保密條款者，廠商應依法求

償。

（十一）廠商履行契約提供及使用之軟體，均需為合法軟體，不得違反智慧財產權、著作權、及專利法之規定，如有違反事情發生，承包廠商須承擔所有法律責任。

（十二）廠商人員從事與本院資訊相關作業時，均須瞭解與遵守本院之資訊安全政策及資訊安全相關規定，並須遵循本案、本院資訊安全管理系統相關規定，本院保留對廠商提供服務之部門、人員、作業進行必要之資安稽核之權利，廠商應保留相關資安紀錄與備份，以配合稽核活動。

（十三）廠商應遵守行政院所頒訂資通安全管理法及施行細則、各項資訊安全規範及標準(如國家資通安全研究院(網址：https://www.nics.nat.gov.tw/.htm)所頒訂之共通規範)，並遵守本院及化學署「資訊安全管理系統( ISMS)」等相關資訊安全管理及保密規定，並應負責處理及通報本院有關本案之資訊安全事件，並依本院所定之安全事件處理及回報程序辦理。廠商如未能即時處理或通報本院，致本院或第三人遭致損失者，廠商應負賠償責任。

（十四）廠商處理個人資料應遵守「個人資料保護法」及相關規定；應記載系統使用紀錄，包括每筆資料之新增/刪除/修改/查詢等資料內容及使用者帳號、時間、IP 位址及事由，並於本院需要時提供相關紀錄。

（十五）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)，並於上線前進行相關原始碼檢測、弱點掃描與壓力測試，應清除正式環境之測試資料與帳號及管理資料與帳號。

（十六）廠商於上線前、保固期末或重大維護修改程式時，應執行網站弱點掃描，及完成弱點修補， 並交付原始碼及 web 網頁資安檢測報告。廠商交付之計畫網站至少應包括跨網站腳本攻擊 (XSS) 及資料庫注入式攻擊(SQL- injection)等開放網路軟體安全計畫(OWASP)所列十大常見網站攻擊模式之測試及防護措施，以保證其提供之系統中不含後門程式、OWASP 十大網路應用系統安全弱點或其他之違反資安之程式漏洞；若經發現，廠商應免費即時移除或更新系統。

（十七）承包廠商須針對支付之系統出具切結書，保證系統內不含後門程式及隱密通道。

（十八）廠商執行本案應依行政院及本院資通安全要求，提供維運系統之網路及資安防護措施相關報告，並執行必要之系統設定及修補等改善措施。

（十九）廠商交付之應用系統應符合 IPv6 之規範，及配合政府組態基準(GCB)之要求進行更新，並提供檢測報告。

（二十）廠商交付之計畫網站應設置於具有保護措拖之環境，保護措拖應至少包括本機防火牆及防護機制，並適時修補系統安全弱點，且應依政府機關(構)資通安全責任等級分級作業規定，定期執行網站弱點掃描，及完成弱點修補，並應依計畫網站盤點及分級評估結果，採行必要之控制措拖，以確保網站之安全防護水準。

（二十一）廠商交付之計畫網站正式運行環境，不得同時作為測試及開發環境使用，並應保存網站建置、維護及更新紀錄。存放機敏性資料應啟用系統存取稽核軌跡記錄功能，且設有存取監控、系統可用性監控及異常警示通報機制。

（二十二）廠商應對本計畫網站資訊系統程式原始碼進行備份，且歷史資料至少保留 3 代或

30 天。（東七機房才有主機網站資料檔案、資料庫及系統環境的備份權限）

（二十三）契約履約或終止後，廠商應刪除或銷毀執行服務所持有本案之相關資料，或依本院之指示返還之，並保留執行紀錄，如有資料外洩致本院或第三人遭致損失者，廠商應負賠償責任。

（二十四）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。

（二十五）廠商提供服務，如發生資安事件時，必須通報本院，提出緊急應變處置，並配合本院做後續處理。

（二十六）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，以符合本院對系統品質及資訊安全的要求。

（二十七）廠商如違反本條款規定，應就本院所受損害負賠償之責；如致他人權利受有損害時，廠商亦應負責。

（二十八）廠商應定期提供本院使用者帳號(作業系統、應用系統與資料庫)與系統存取權限審查紀錄。

（二十九）廠商應於專案結束時，提供程式源碼予甲方，含完整檢測及版本控管紀錄。

（三十）廠商依資通安全管理法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務）應注意事項如下：

1. 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。
2. 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。
3. 廠商辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之廠商應具備之資通安全維護措施。
4. 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。
5. 受託業務包括客製化資通系統開發者，廠商應提供該資通系統之安全性檢測證明；涉及利用非廠商自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
6. 廠商執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
7. 廠商應採取之其他資通安全相關維護措施。

（三十一）本院依資通安全管理法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督廠商時應注意事項如下：

1. 委託關係終止或解除時，應確認廠商返還、移交、刪除或銷毀履行契約而持有之資料。
2. 委託機關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。
3. 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等

級及內容，就執行該業務之廠商所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項：

(1)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)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)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。

（三十二）廠商交付之應用系統應具有輸入資料之檢核，敏感資料之加密及適切之權限管制設計，另於上線前進行系統測試，並提供相關測試之報告。

（三十三）廠商保證其於受託期間以及本案終止後，在未取得機關之書面同意前，不得向任何人、單位或團體透露任何業務上需保密之文件及資料，並配合機關規劃參與資安教育訓練。廠商保證於契約終止（或解除）時，應交還本院所屬財產，及在履約期間所持有之需保密之文件及資料。

## 附件二、個人資料保護條款

廠商依本契約受本院委託蒐集、處理或利用個人資料及檔案（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等等個人資料保護法所指個人資料）時，廠商應遵守下列約定：

（一）蒐集、處理或利用時之義務

1. 廠商基於本契約蒐集、處理或利用個人資料時，應符合個資法、化學署及所屬機關個人資料保護管理要點等相關規定。
2. 廠商基於本契約蒐集、處理或利用特種個人資料時，應遵守個資法及化學署及所屬機關個人資料保護管理要點等相關規定，並檢附符合個資法第六條第一項但書各款任一要件之說明。
3. 廠商不得利用本院所提供或因執行本契約所蒐集個人資料及檔案，為自己或他人利益從事本契約委託範圍以外之處理或利用行為，包括但不限於行銷或商業推銷等相關活動、連結比對廠商本身保有資料進行處理利用，或以任何方式或方法交付予履約無關之第三人。
4. 廠商僅得於本院以下指示之範圍內，蒐集、處理或利用個人資料：
   (1)本院保留指示之事項。
5. 廠商認為本院之指示有違反個人資料保護法、其他法律或其法規命令者，應立即通知本院。

（二）安全管理措施

1. 廠商在執行業務所必需之範圍內，應依個資法之安全管理措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。
2. 前目安全管理措施應包含下列事項，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。
   (12)其他機關書面指示業務執行應注意事項。

（三）當事人權利行使時之義務

本院若受理當事人依個資法第三條規定行使當事人權利時，廠商應於本院指定期限內，配合提供必要資料或說明；當事人若逕向廠商及其受託人行使個資法第三條所定權利者，廠商及其受託人應依相關規定予以答覆，於有疑義時應通知本院協助處理，並留存所有紀錄以供機關查核。

（四）配合義務

1. 廠商依個資法第十五條第二款或第十六條但書第七條規定，經當事人同意而為蒐集或特定目的外利用時，就該同意內容與取得方式應事先送交本院審查。廠商依個資法第六條第一項第六款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。
2. 本院於本契約期間內，得要求廠商提供或說明涉及個人資料業務之處理流程相關資料（包括但不限於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、利用等相關資料），廠商不得拒絕。

（五）緊急事故通知義務

廠商有因執行本契約，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，應立即通知本院並採取因應措施，以避免或降低損害範圍；廠商於查明後應將其違反情形、涉及個資範圍、採行及預訂採行之補救措施，經本院同意後，依法以適當方式通知當事人。

（六）定期確認

1. 本院得針對廠商的個人資料安全管理措施實施情形進行確認，並將確認結果紀錄之；必要時，得派員進行實地訪查或委託專業人員進行查核，廠商應予配合。
2. 本院於訪查或查核後，認有缺失，得以書面敘明理由請廠商限期改善。

（七）損害賠償責任

1. 廠商違反本契約任一條款，本院提出限期改善建議，廠商未依期限改善時，機關得依情節輕重為以下的處理；若本院受有損害，並得請求損害賠償：
   (1)以書面通知廠商終止或解除契約之部分或全部。
   (2)要求減少部分或全部價金。
   (3)按契約總價的千分之 1.5，計收懲罰性違約金。
2. 廠商因執行本契約業務而違反個資法、個資法施行細則等規定，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。
3. 本院如因廠商執行本契約而違反個資法、個資法施行細則，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，廠商應協助機關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，並負責清償本院因此對第三人所負之損害賠償責任）

（八）履約中或契約終止時資料之刪除或返還

1. 除本院、廠商雙方另有約定或法律另有規定外，廠商應於受託執行業務期間屆滿或經本院要求時，將因履行受託業務而取得之個人資料及檔案全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷燬或返還個人資料之時間、方式、地點等紀錄。

2. 前目返還，廠商得以交付機關指定之第三人為之。
3. 第一目刪除、銷毀作業，機關於必要時，得實地查訪，廠商應予配合。

## 附件三、保密同意書

# 保 密 同 意 書

茲緣於簽署人.....簽署人姓名，以下稱簽署人參與.....（廠商名稱，以下稱廠商 得標**環境部化學物質管理署**（以下稱機關）資訊業務委外案.....（案名））（以下稱「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，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人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 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。 簽署人同意公務秘密與業務秘密，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。

第三條 簽署人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 簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關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，簽署人及其任職之廠商亦應負賠償責任。

第五條 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。

第六條 本同意書一式叁份，機關、簽署人及.....廠商）各執存一份。

簽署人姓名及簽章

身分證字號：

聯絡電話：

戶籍地址：

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

**附件四、保密切結書**

# 保 密 切 結 書

立切結書人____（簽署人姓名）等，受_____（廠商名稱）委派至**環境部化學物質管理署**處理業務，謹聲明恪遵機關下列工作規定，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，均保證善盡保密義務與責任，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，絕無異議。

一、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。

二、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。

三、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，須提交病毒、漏洞或後門程式檢測報告予本署確認後始能為之。

四、廠商駐點服務及專責維護人員原則應使用該廠商配發之個人電腦與週邊設備，並申請使用機關內部網路。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。

五、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。

六、本保密切結書不因立切結書人離職而失效。

七、立切結書人因違反本保密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。

**立切結書人：**

中文姓名及簽章：_____ 護照英文姓名：

身分證字號：_____ 出生年月日：_____ 聯絡電話：

戶籍地址：

駐在（承辦）單位：_____ 科別：___ 卡號：___ 分機：

**立切結書人所屬廠商：**

廠商名稱及蓋章：_____ 廠商負責人姓名及簽章：

廠商聯絡電話：_____ 地址：

**填表說明：**

一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中 華 民 國　　年　　月　　日