財團法人保險事業發展中心

全球資訊網資安防護升級暨功能增修案

需求說明書

中華民國114年11月

目錄

[第一章 專案概述 2](#_Toc210837997)

[第一節 專案名稱 2](#_Toc210837998)

[第二節 專案目的 2](#_Toc210837999)

[第三節 專案範圍 2](#_Toc210838000)

[第四節 專案時程 2](#_Toc210838001)

[第二章 環境說明 3](#_Toc210838002)

[第三章 應用系統需求 5](#_Toc210838003)

[第一節 功能性需求 5](#_Toc210838004)

[第二節 資安需求 5](#_Toc210838005)

[第三節 程式開發與設計需求 11](#_Toc210838006)

[第四節 教育訓練需求 12](#_Toc210838007)

[第四章 系統測試 13](#_Toc210838008)

[第五章 專案管理 14](#_Toc210838009)

[第一節 時程規劃 14](#_Toc210838010)

[第二節 交付項目 14](#_Toc210838011)

[第六章 系統維護與保固 16](#_Toc210838012)

1. 專案概述
2. 專案名稱

全球資訊網資安防護升級暨功能增修案，以下簡稱「本專案」。

1. 專案目的

本中心「全球資訊網」（以下簡稱本網站）於105年改版升級啟用至今已逾多年，本網站核心架構版本於115年將停止支援，為強化本網站之資安防護功能以因應近年資安威脅提升，亦符合本中心資通安全責任等級之相關規範可確保資訊安全，並配合業務單位可自行更新資料至本網站等功能增列等需求，為優化本網站功能，規劃本專案進行全球資訊網資安防護升級暨功能增修。

1. 專案範圍
2. 「全球資訊網」（含員工專區系統)之功能開發及優化。
3. 本系統驗收合格日次日起一年保固維護。
4. 本系統之教育訓練。
5. 專案時程

得標廠商須於115年11月02日(含)前完成本專案系統上線作業。

1. 環境說明

正式環境與測試環境之軟硬體設備及網路架構環境由本中心提供。

1. 主機資源，包含網頁服務主機、應用系統服務主機及資料庫主機

正式環境

| 設 備 | 數量 | 中央處理器/部 | 記憶體/部 |
| --- | --- | --- | --- |
| 資料庫虛擬主機  DB Server | 1部 | 2 Core、時脈2.0 | 40GB |
| 應用系統服務虛擬主機  AP Server | 1部 | 4 Core、時脈2.0 | 12GB |
| 網頁服務虛擬主機  Web Server | 1部 | 2 Core、時脈2.0 | 8GB |

測試環境

| 設 備 | 數量 | 中央處理器/部 | 記憶體/部 |
| --- | --- | --- | --- |
| 資料庫虛擬主機  DB Server | 1部 | 2 Core、時脈2.0 | 16GB |
| 應用系統服務虛擬主機  AP Server | 1部 | 4 Core、時脈2.0 | 8GB |
| 網頁服務虛擬主機  Web Server | 1部 | 2 Core、時脈2.0 | 8GB |

1. 系統軟體

| 設 備 | 設置地點 |
| --- | --- |
| Tomcat 9.0 | 正式環境、測試環境 |
| Java 21 | 正式環境、測試環境 |
| 前端主機作業系統  windows server 2022 | 正式環境、測試環境 |
| 資料庫主機作業系統  MSSQL 2022 | 正式環境、測試環境 |

1. 應用系統需求
2. 功能性需求
3. 強化資安防護能力(程式語言版本與opencms版本升級)
   * 1. 「全球資訊網」(含後台)核心
     2. 員工專區系統(含後台)核心
4. 功能增修:
5. 「全球資訊網」－統計報表上傳功能

(首頁>精算統計>壽險財業務統計-一般民眾)

建立統計報表上傳功能，可更新報表最新內容及下載。

1. 員工專區系統－國際期刊上傳功能

建立國際期刊上傳功能，可更新研究報告最新內容及下載。

1. 資安需求
2. 系統開發安全需求
3. 本案之應用系統開發過程應遵循安全軟體開發生命週期(SSDLC)，以確保所有之應用程式皆在應有之安全功能下執行，並應參考「國家資通安全技術服務與防護管理計畫-Web應用程式安全參考指引」，以強化應用系統的安全。
4. 為考量應用系統安全，承包廠商應提具本案所採用之共同安全模組，並確保所有應用程式皆在此共同安全模組下執行。
5. 本案所開發或修改之程式應使用OWASP (code review)以及應用程式安全測試紀錄應留存測試檢驗之軌跡，以資佐證。若有系統檢測漏洞應限期改善，經參考開放Web軟體安全計畫(OWASP)評定之風險等級，屬高風險以上者應於3個禮拜內修正完成(與本中心協調另行約定修補時間者不在此限)，其餘弱點依照本中心TII-ISMS-B-007\_通信與作業管理程序書規定辦理修補。
6. 程式開發需避免已知之弱點，如OWASP最新前十大安全問題列表，或未來發佈之安全問題列表。
7. 原始碼檢測及弱點掃描報告內容需包含下列項目：（最多）前30高風險主機列表（含高、中、低風險數）、高、中、低風險弱點數量與比率、各類型弱點數之統計圖、各主機發現的弱點列表（依高、中、低風險排序）、各主機弱點說明、建議與相關資訊。
8. 若遇有系統重大更新時，本中心得視該重大更新對專案之影響程度，要求承包廠商針對影響所及之部份，增辦程式碼審核或網站弱點掃描測試，經測試安全無虞後，始得正式上線。
9. 廠商須於本專案範圍內，須無償配合本中心資安相關規範辦理應用系統弱點修補及異常排除。
10. 廠商須確保所有非公開資訊均必須於帳號登入後才能進行查詢、增修、刪除、下載。
11. 廠商須提供管理人員使用權限控管。
12. 廠商必須進行適當設定，防止一般使用者因系統設定不當，藉由網頁方式瀏覽目錄，進而獲得系統檔案資訊及進行破壞。
13. 非經本中心同意，廠商不得擅自作為對外提供；如有竊取公務資訊，如涉及違法洩密造成本中心損害者，廠商與服務人員均須負民、刑事法律賠償責任。
14. 廠商應使用輔助管理工具，對專案建構之服務項目進行安全控管，以確保資訊系統之正確性。各應用系統包括原始程式碼、軟體文件、測試資料、工作手冊等，均應妥善保存。
15. 廠商應確保開發及維護之軟體系統中，無植入木馬程式、後門程式或任何有危害資訊安全之程式碼，以免危害未來系統及資訊安全，否則應負一切法律責任並賠償本中心損失，如為維護人員個人行為，廠商亦應負連帶責任。
16. 應用系統開發設計時，需將應用程式的安全納入考量，避免駭客可利用例如緩衝區溢位、資料隱碼(SQL Injection)、XSS、錯誤訊息等得到入侵的資訊。
17. 網頁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。
18. 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。
19. 程式失敗時，可能產生的錯誤碼應交由例外程式處理(Exception handling)。
20. 網頁開發完成上線後，應提供一份可執行之完整版本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作為備份或因應緊急復原時使用。
21. 廠商執行維護作業，如版本更新、異動資料檔或變更設定等，應遵循本中心資訊安全管理要求提出需求變更，並經系統管理人員審核後始得進行變更事宜，相關紀錄應留存備查。
22. 系統安全設計
23. 網頁應限制未經合法登入無法由URL直接開啟。
24. 應用程式不得使用作業系統(如Windows、Linux、AIX等)管理者(如administrator、root等)為登入帳號，亦即不以管理者帳號登入即可正常運作，且作業系統系統管理者(如administrator、root等)密碼改變亦不影響其應用程式正常功能。
25. 資料庫連線帳號不得使用資料庫系統(如SQL、ORACLE、MySQL等)管理者(如 sa、dba等)為登入帳號即可正常運作，且資料庫系統管理者(如sa、dba等)密碼改變亦不影響其應用程式正常功能。
26. 如系統對於有關使用者權益或必須遵循一定的流程作業，應避免使用者使用瀏覽器之「回上一頁」功能，回上一畫面修改資料並存檔，而產生資料不一致現象。
27. 應用程式如有部分功能需權限控管或有條件判斷(如勾選放棄則不能再執行後續的資料填寫)，應於進入頁面時進行狀態檢查。
28. 應設計使用者登入檢核機制，並顯示適當之訊息提供使用者知悉使用者登入行為(含登入成功與失敗)。
29. 應設計連線(Session)控制及網頁逾時(TimeOut)中斷機制，使用者超過十五分鐘未使用應中斷其連線或採取其他保護措施。
30. 系統任何錯誤訊息，必須妥適處理，避免對外顯示敏感訊息。
31. 資料安全需求
32. 利用網際網路傳輸之資料，需以SSL機制進行加解密。
33. 系統必須防止資料隱碼(SQL Injection)、Cross Site Scripting(XSS)等攻擊與防止使用者在網址列輸入網址及帶參數方式以別的使用者帳號進入系統網頁破壞、新增、修改、刪除、查詢及列印系統任何資料。
34. 為符合個資法要求，承包廠商需提供資料庫軌跡留存租賃服務，相關軌跡需保留五年。
35. 為提升資料儲存機密性，本案資料庫實體檔案需啟用加密功能。
36. 系統安全需求

承包廠商需提供相關管理作業機制、程序供後續查核使用。相關安全需求如下：

1. 具有系統管理權限者之系統管理及資料存取，需有稽核軌跡以利查核且均應獨立存在。
2. 系統管理權限必需有角色分離的制衡機制，即系統管理者不可兼任資料庫管理員。
3. 主機的特權及高權限帳號的使用應透過特權帳號管理系統控管，並套用政府組態基準(GCB)強化密碼強度，專案人員透過申請取得作業使用之密碼。
4. 營運環境如遇分散式阻斷服務攻擊時，應具備流量清洗服務。
5. 營運環境的應用系統版本更新應有人工管理程序審核，確保系統安全。
6. 資安事件監控管理服務需求
7. 資安事件分類與分級，應同時參照行政院國家資通安全會報頒布之「政府機關（構）資訊安全責任等級分級作業實施計畫」之分級標準及本中心「安全事故緊急應變程序書」之摘要重點為原則，以相同定義進行維運。
8. 承包廠商需根據資安事件類型及資安事件發生所在之資訊安全架構區塊，以及資安事件發生所造成之影響等級（參考數位發展部發佈之「資通安全事件通報及應變辦法」），建立關連分析規則，於發生資安事件時，需能即時通報，進行事件處理工作。
9. 提供因應個資法之顧問及支援，包含數位鑑識之技術發展、制度管理、資料保存及舉證免責等。
10. 資訊安全分析需求

承包廠商於專案合約期間內，所有資安檢測作業必需由本中心認可，並出具測試報告。

1. 資安檢測與防護
2. 需提供本系統持續性程式異動監控，並妥為應變處理(如：告警及程式復原等機制)，本專案驗收或每次上版至營運環境前需進行原始碼掃描，同時本專案驗收時需提交原始碼檢測及弱點掃描報告。
3. 本專案系統之資通安全防護需求等級屬中級，廠商之相關防護機制(如存取控制等)請依「資通安全責任等級分級辦法」所訂之「資通系統防護基準」辦理，並填寫「資通系統防護基準檢核表」。
4. 本專案廠商應配置資通安全專責人力1名。
5. 程式開發與設計需求
6. 本專案採Java開發，如有需要使用其他程式語言之必要者，應先提報本中心，經本中心同意後使用。
7. 廠商應交付完整原始程式碼(source codes)，並視本中心需要，建立內部管理機制。若需採用第三方元件或程式庫，應於系統設計階段提出，經本中心同意後使用，可不提交前揭原始程式碼，惟須提交第三方元件清單及使用說明文件。
8. 字碼處理應採UTF-8編碼方式。
9. 應提供版本控管機制。
10. 對外網站應採用響應式網頁設計(Responsive Web Design, RWD)，當使用不同顯示尺寸之電腦、平板及智慧型手機等裝置瀏覽時，因應不同解析度動態調整網頁版面配置。
11. 資料庫規劃與設計
12. 廠商應針對資料庫管理機制進行相關設計，如建置規範、命名規則、資料庫權限管理機制等。
13. 廠商應配合現行資料庫監控機制，記錄相關日誌(Log)並提供查詢功能。
14. 如經資料庫監控作業，發現有不當消耗CPU資源或記憶體之SQL陳述，廠商應配合進行調校。
15. 教育訓練需求
16. 訓練內容

針對本中心之使用單位與資訊人員，廠商應配合需求提供相關訓練課程，課程內容應包含系統簡介、系統操作、系統管理等項目，本中心得調整課程內容與訓練人數，系統操作教育訓練須配合本中心和產險公司、銀行使用單位與資訊人員之訓練需求。

1. 訓練方式

教育訓練師資、時程及場地須與本中心討論，並經確認同意後進行教育訓練。

1. 訓練時間

於專案上線前或保固期間依業務需求，由本中心與廠商協定。

1. 系統測試
2. 系統測試
3. 測試作業範圍說明如下：

|  |  |  |
| --- | --- | --- |
| 測試項目 | 測試單位 | 環境 |
| 單元測試 | 廠商 | 開發環境 |
| 功能測試 | 本中心 | 測試環境 |

1. 各功能範圍依據上表於不同環境分別執行「單元測試」及「功能測試」，於測試前應檢附「測試計畫」並經本中心確認後據以實施。測試範圍、方式及驗證標準原則說明如下：

| 測試標的 | 測試範圍 | 測試方式及驗證標準 |
| --- | --- | --- |
| 系統功能 | 詳「第二章、第一節 功能性需求」 | * 測試方式   於「測試環境」測試。   * 驗證標準   與測試計畫書所述之輸出說明比對一致。 |

註：以上所描述之測試方式係以測試「功能面」是否正確，若是因不正常資料所引起，經人為判斷若新系統結果正確，則該測試個案以通過計之。

1. 專案管理

專案須依本中心「TII-ISMS-B-009\_系統開發與維護管理程序書」執行，本中心得視需要招開專案工作會議。

1. 時程規劃

本專案於合約生效日起至於115年11月02日(含)前完成系統上線，各階段規劃時程如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項次 | 辦理事項 | 說明 | 配合對象 | 專案時程 |
|  | 系統測試 | 測試機測試 | 保發中心 | 115年07月15日  至  115年10月15日 |
|  | 系統上線 | 正式機上線 | 保發中心 | 115年11月02日(含)前 |
|  | 教育訓練 | 於專案上線前或保固期間依業務需求，由本中心與廠商協定 | | |

1. 交付項目

應於本專案申請驗收前提交下列文件各3套。文件形式包括紙本書面文件及電子檔(光碟片)，須為MS之Word檔案格式。

本專案所開發之軟體，須提供原始程式碼3套(光碟片，內含程式清單)，作為系統維護之用，若為廠商自行開發之共用軟體元件或套裝產品，得不提供原始程式碼，但需免費提供安全性更新服務。

| 項次 | 階段項目 | 交付時程 |
| --- | --- | --- |
| 1 | 軟體需求規格書  (含需求訪談) | 115年11月02日(含)前 |
| 2 | 軟體設計規格書(含資料庫設計調整) |
| 3 | 軟體測試計畫書 |
| 4 | 軟體測試報告  (含系統測試、原始碼檢測、弱點掃描) |
| 5 | 系統操作手冊  (含教育訓練教材) |
| 6 | 原始程式碼 |

1. 系統維護與保固
2. 自驗收合格日次日起，得標廠商應提供一年免費之維護保固。
3. 在本專案契約保固期間內，因應實際業務需要而需調整系統功能所增修之程式與系統文件，在系統功能數10%範圍內(以程式新增支數計算)，不另付費予廠商；程式增修支數認定原則為每修改6支程式，視同增撰1支程式，其逾10%部分，得另案就相關功能項目之價金，按變更比例給付價金。
4. 保固服務期間，廠商應指派專人彙整本中心所提出之問題需求，辦理資訊系統維護工作，業務單位提出之修正或增修功能，由雙方協議訂定完成時程。
5. 廠商應配合前項系統增修作業，於保固到期日前交付最新版本之軟體設計規格書及系統操作手冊紙本3份及光碟各3份。
6. 保固服務期間，廠商進行程式修改或資料庫調整，均須依據本中心資訊安全及個人資料管理制度(ISMS及PIMS)規定辦理。
7. 在本專案保固期間，廠商應依本中心要求，辦理資訊技術移轉及應用系統教育訓練，以協助本中心作系統維護服務。
8. 得標廠商進行系統維護工作時，如與其他廠商負責之部分相關，則應明確提供其他廠商或本中心應配合之作業項目，如有爭議，本中心對責任歸屬確認具解釋權。
9. 得標廠商進行各項維護作業時，應留存完整書面或電子紀錄。
10. 廠商於本保固範圍內，須應本中心需求無償配合本中心對災害復原機制進行相關演練事宜。
11. 在本專案合約期滿或終止時，廠商必須辦理資訊技術移轉及應用系統教育訓練並確保專案資料之完整，以協助本中心人員或接替廠商進行後續系統維護服務。