「IEK 廣告系統安全性與效能優化專案」規範書

壹、 專案目標

IEK 廣告系統主要提供 IEK 產業情報網寄送會員電子報、研討會等各項活動通知，自建置及上線啟用迄今，已歷多年未進行改版，因此進行本優化與安全性專案，專案目標如下：

1. 系統改寫：.Net Framework 2.0 程式改寫編譯為 .Net Framework 4.8 或以上
2. 效能調整：前端廣告與後端統計頁面載入效能優化調整
3. 資安修改：白箱與黑箱掃描風險項目調整
4. 拓展應用：產生嵌入式 Scripts 供 IEK 外部合作夥伴網站系統使用，以提升情報網露出及流量來源；跨 Domain 及惡意使用的資安限制與防護做法

貳、 專案時程

一、於 2026/12/20 前，完成系統程式開發，並交付工研院安裝測試與上線。

參、 系統設計與功能需求

一、IEK 廣告系統置放於「IEK 產業情報網 -後端功能 -全站廣告管理」功能內：



二、服務功能架構：

1. Banner 廣告：

   i. 現有圖片型版位管理功能改寫與效能優化

   ii. 現有圖片型廣告管理功能改寫與效能優化

2. 快訊：

   i. 現有快訊設定管理功能改寫與效能優化

   ii. 現有快訊發佈功能改寫與效能優化

3. 文字型資訊：

   i. 現有文字型區塊管理功能改寫與效能優化

   ii. 現有文字型廣告管理功能改寫與效能優化

4. 圖文型資訊：

   i. 現有圖文型區塊管理功能改寫與效能優化

   ii. 現有圖文型廣告管理功能改寫與效能優化

5. 產生嵌入 JS

   i. 現有嵌入 JS 頻道內容改寫與效能優化

   ii. 新增拓展應用：產出可提供外部第三方網站嵌入使用的 JS

   iii. 拓展應用 JS 中需求上述 1、3、4 項廣告資訊的新增與維護，請增加相對應的內容維護選項與功能

6. 數據統計

   i. 數據統計頁面改寫與效能優化

   ii. 包含各項廣告資訊的統計資訊

   iii. 數據統計頁面的排版調整

7. 須滿足安全性與權限設計：

   i. 支援 IEK 產業情報網的權限控管

   ii. 第三方網站嵌入 JS 的資安限制與安全防護設計，避免惡意使用，影響 IEK 產業情報網正常營運

iii. 所有傳輸需透過 HTTPS

三、其他需求：

1. 開發須採用原本系統之程式開發架構，不得任意變更；若有新增架構需與本部門系統負責人進行討論並經同意後，方可調整。

2. 系統需遵循原有的資料交換標準與格式，不得任意變更；若需調整原有功能的處理邏輯需與本部門系統負責人進行討論並經同意後，方可調整。

肆、 系統開發規範

(一)工具與環境

1、 既有功能調整：
現行版本為 .Net Framework 2.0，需求改寫編譯為 .NET Framework 4.8 或以上版本及相關工具，並確保程式架構功能正常運作。

2、 新功能開發與後續維護：
一律採用下列環境（或更高版本），並確保支援 .NET Framework 4.8 或以上：

- 開發工具：Microsoft Visual Studio 2026
- 資料庫：Microsoft SQL Server Standard 2025(64-bit)
- Web Server：Windows Server 2019 + IIS 10.0

(二)付費軟體限制

不得在開發、測試、部署或維運流程中使用任何需額外授權費用的商業軟體、元件或雲端 SaaS 服務。

(三)第三方免費／開源軟體使用原則

1、 使用任何免費或開源（FOSS）軟體前，須取得系統負責人核可

2、 僅允許 MIT、Apache 2.0、BSD 等可商用且無授權衝突之條款

3、 未經核准擅自引入之第三方套件，一經查獲，供應商須於限定期限內移除或替換，

並承擔相關時程延誤與成本責任

(四)程式目錄架構通則

依循現有程式目錄架構。

(五)系統相關命名規則

1、 **一般原則**(採用 CAMEL 方式)：
即名稱由多個 word 組成時，word 與 word 中間不以其他字元區隔，第二個 word 後之 word，該 word 之第一個字母為大寫，其餘字母為小寫。

2、 **變數名稱**：型別 prefix + 有意義名稱

3、 **ADO.NET 變數名稱**：ADO Object Prefix + 有意義名稱。

伍、 系統建置規範

(一)伺服器端：程式需在下列環境下執行：

1. Microsoft IIS 10.x 以上 with .Net Framework 4.8.X。

2. Microsoft SQL Server 2025。

(二)用戶端：應用程式需在下列瀏覽器中正常運作：

1. Microsoft Edge 156.x 以上。

2. Google Chrome 156.x 以上。

(三) 承包廠商發展平台必須符合本專案之作業平台規範。承攬廠商需承諾程式原始碼不含特洛伊木馬程式(Trojan code)或其它危害資訊安全項目。請參考「工研院網頁網站程式規範」。

(四)網頁相關之圖示、圖形、技術與程式碼之來源必須符合著作權法之規定，若有違反，一切法律責任必須由得標廠商自行負責。

(五)技術需求：業者必須有足夠技術確能實際參與解決 Web 主機系統及網路技術問題。

(六)環境需求：環境須能與工研院現有軟體設備相容。本案各項網頁資料內容以及資料展現、維護及管理制程式均須建置於本單位指定之軟硬體環境。

(七)系統維護：業者必須參與實際維護工作及問題解決。須將資料及技術移至工研院。各系統上所有相關元件，工研院擁有永久使用及修改權。

(八)交付產品：完成之作品，完成產品放置本單位指定之場地安裝測試合格驗收交付電子檔案資料留置工研院。

(九)權利歸屬：承包廠商開發並安裝於本單位指定設備之應用程式應提供原始程式碼，工研院擁有其智慧財產權、所有權及修改權，工研院得自行複製安裝做加值運用。廠商如涉及仿冒侵權及洩密情事，違反有關法令，而造成本院之損失，或致工研院負民刑事責任時，廠商應賠償本單位一切損害（包含但不限於訴訟及律師費用等）。

(十)工作成果(如程式、說明文件、報告等)所有權歸工研院所有。

(十一) 廠商需保證對工作成果之使用不會侵害或違反任何第三人之專利、著作權、商業機密、契約權利或其他專有權利，若因違反而造成損害，承包廠商應負一切損害賠償責任。

(十二) 非經工研院書面同意，承包廠商不得對外揭露其執行作業或作業過程中獲悉之任何資料，若因違反而造成損害，承包廠商應負一切損害賠償責任。

(十三) 本系統中不得含有惡意竊取個人或公司資訊的程式碼，並遵守中華民國「個人資料保護」相關法令規定。若因違反而造成損害，承包廠商應負一切損害賠償責任。

陸、 驗收規範

廠商必須於 2025 年 12 月 20 日前，完成並交付開發完成之系統程式碼，並完成安裝於工研院測試主機中。若逾期不能交付開發完成之程式碼，每逾一日，罰總成交金額千分之一，罰款上限為成交總金額之百分之二十。另外，系統負責人得視專案需求，要求承包廠商辦理教育訓練。交付程式碼時，須附交下列（但不限於）相關文件，並依工研院 ISO 文件格式製作：

1. 程式清單與功能說明
2. 資料字典

附件一：工研院網頁網站程式規範

一、IIS Web Server 平台程式存放規則：

1. Server 版本

    1. Microsoft (Windows 2019 以上) 英文版 + 中文 CodePage。

    2. Internet Information Server(IIS) 10.0。

2. 已支援的元件及技術

    1. ADSI 5.2.3790 版(Windows 2003)。

    2. ADO 2.7、OLD DB 4.0、ODBC 3.51(MDAC 2.8)。

    3. XML、XSL，Parser 為 MSXML Parser，版本支援 6.0 版。

    4. 支援 ASP.NET 環境(.NET framework 版本為 4.8 以上)。

    5. 支援 Ajax 2.0 以上

3. 不支援的元件及技術

    1. 不開放使用 MTS/COM+ 。

    2. 不支援 Microsoft Message Queue。

    3. 不開放 IIS 之 SMTP Service。

    4. 不支援匿名存取者(anonymous)可存放資料的資料庫，如 Access 等。

    5. 不支援 Java Servlet/Java ServerPages。

    6. 不支援 php(可至 Linux 平台申請)。

4. 組態設定

1. Web 應用程式可要求設定虛擬目錄(Virtual Directory)，但虛擬目錄下不可再設定虛擬目錄(若目錄名稱與欲使用的虛擬目錄相同，可以申請直接設定成Application)。

2. Web 應用程式上線時，不可要求設定成服務(Service)。

3. 如需使用虛擬站台(Virtual Site)，請於申請時提出，並一併告知欲使用之Domain Name。若 Domain name 不採用 *.itri.org.tw 時，使用者需自行向財團法人台灣網路資訊中心(http://www.twnic.net.tw)所授權之機構申請(ie:中華電信,數位聯合...等)，並可請林軒宇先生(分機 18080)代辦 Domain Name 之申請。

4. 網頁存取權限預設為 anonymous（匿名）可存取(Read Only)，若需採認證，必須於申請時一併註明。

5. IIS Web Server 目前提供基本驗證(Basic authentication)、整合的 Windows 驗證(Integrated Windowsauthentication)及牆 Single Singn On(SSO)，唯 SSO 僅支援牆內，牆外不支援(若牆外網站有此方面需求請洽管理人員尋求協助)

6. 網站(目錄)預設頁面，搜尋順序設定為 index.htm、index.html、index.asp、index.aspx、defautl.htm、default.html、default.asp、index.aspx。

7. IIS Server 支援下列附檔名的應用程式對應：*.asp,*.aspx, *.asa, *.cer, *.cdx, *.shtm, *.shtml, *.asax, *.ascx,*.ashx, *.asmx, *.axd, *.rem, *.soap, *.config, *.webinfo, *.licx, *.resx, *.resources, *.vsdisco。

5. 程式開發注意事項

1. Web 應用程式開發，需符合資訊中心訂定以 Microsoft Edge 版以上為程式開發標準環境之規定。

2. 若發現有洩露系統資訊或危及系統安全之程式，系統管理員有權立即停止該 Web 空間使用權。

3. 為避免影響 Web Server 上其他網頁或站台，Web 應用程式上線時，不可要求重新開機或重開 Web Service。

4. Web 應用程式上線時，基於系統安全考量應用程式檔案應放於系統管理員所告知的目錄下，不可要求置於$SYSTEMDRIVE\inetpub\scripts 或 $SYSTEMDRIVE\inetpub\wwwroot 中。

5. 程式撰寫時，若需對 Server 做 Write 的動作，檔案需另外放置於指定目錄中，以免造成安全性的漏洞，且該目錄應不在 IIS 可以控制的目錄中。所有檔案的寫入和讀取必須自行以程式控制。

6. 若程式有進行寫入的動作，則程式針對此動作必須進行身份認證的動作。Intranet 的網站建議使用 Domain 做為認證來源(Windows 基本認證)；Internet 網站如果是對外要求認證，可以自行寫程式控制；如果是對內部同仁要求認證，亦可使用 Windows 基本認證。

7. 若需開發檔案上傳功能，不建議使用 Microsoft 的 Posting Acceptor。ASP.NET 的網頁建議直接使用 .NETFramework 提供之 class(System.Web.UI.HtmlControls.HtmlInputFile)來處理上傳檔案。

8. 若需使用資料庫，請使用 MS SQL Server 資料庫，不允許使用 File Base 的資料庫(如 MS Access)。

9. 由於 IIS Server 不開放 SMTP Service，若要寄送 E-mail，請直接利用程式將 mail 送往 pnmail.itri.com.tw(上線區); mail.itri.org.tw(測試區)。

10. 由於 IIS Server 不開放 Index Service，如需使用 Search 功能，須另行申請。

11. Web 應用程式若須使用資料庫，不可使用 SA 或具有 DBO 權限的帳號進行連線。

12. 當程式欲連結資料庫時，建議採用 DSN-LESS 的模式進行連結。

6. 其他注意事項

1. 網頁採透過院內電腦資料夾分享(File Sharing)的方式上傳，不支援網頁編輯軟體透過 FTP 直接發送網頁至 IISWeb Server(也就是不開放 FTP)。

2. 除以上所列支援程式外，其餘應用程式均不支援（例如，不支援 Office）。

3. 若所使用之技術、元件不在上述清單中(或是版本不合)，一律視為不支援，若有任何需求，請於一個月前提出申請。

4. 上線程式須將 debug mode and tracing 設為 off。

二、Web 用 SQL Server 程式存放規則

A. SQL Server 版本

1. Microsoft Windows 2019。

2. MS SQL 2025 設定為 CHINESE_TAIWAN_STROKE_BIN

B. 資料庫 Data Dictionary 原則

1. Table Name 及 Field Name 需採用英文名稱，不得使用中文名稱。

2. 由 Web 程式連接時，禁止使用 SA 或具有 DBO 權限的帳號。

3. 資料欄位名稱、資料表(Table)名稱，必須區分大小。