ടെലിഫോൺ നമ്പർ : 2512524
പോസ്റ്റ് ബോക്സ് നമ്പർ : 5430
ഫാക്സ് : 0471-2305891
പിൻ കോഡ് - 695 033

ഇ-മെയിൽ: secretary@niyamasabha.nic.in

കേരള നിയമസഭാ സെക്രട്ടേറിയറ്റ്

നം : KLS/15070/2024-Ac D2

തിരുവനന്തപുരം
28.09.2024

താൽപര്യപത്രം

നിയമസഭാ നടപടികളുടെ പരിഷ്കരിച്ച വെബ്കാസ്റ്റിംഗ് സോഫ്റ്റ് വെയറിന്റെ സെക്യൂരിറ്റി ഓഡിറ്റിംഗ് നിർവ്വഹിക്കുന്നതിനായി സംസ്ഥാന സർക്കാരിന്റെ ഐ.ടി. സംബന്ധമായ പ്രവൃത്തികളുടെ നോഡൽ ഏജൻസിയായ ഐ.ടി. മിഷൻ ലിസ്റ്റ് ചെയ്തിട്ടുള്ള സ്ഥാപനങ്ങളിൽനിന്ന് (CERT-IN Empanelled Agencies) താൽപര്യപത്രം ക്ഷണിക്കുന്നു.

താൽപര്യമുള്ള സ്ഥാപനങ്ങൾ അവരുടെ സ്ഥാപനത്തെ സംബന്ധിച്ച വിവരം, ഈ മേഖലയിലെ പ്രവൃത്തി പരിചയം, ബന്ധപ്പെട്ട മറ്റ് വിശദാംശങ്ങൾ എന്നിവ വിശദമാക്കുന്ന താൽപര്യപത്രം **03.10.2024 രാവിലെ 11.00 മണിക്ക്** മുമ്പായി അണ്ടർ സെക്രട്ടറി II (അക്കൗണ്ട്സ്), നിയമസഭാ സെക്രട്ടേറിയറ്റ്, തിരുവനന്തപുരം-33 എന്ന വിലാസത്തിൽ എത്തിക്കേണ്ടതാണ്. താൽപര്യപത്രം ഉള്ളടക്കം ചെയ്ത കവറിന് പുറത്ത് **"നിയമസഭാ നടപടികളുടെ പരിഷ്കരിച്ച വെബ്കാസ്റ്റിംഗ് സോഫ്റ്റ് വെയറിന്റെ സെക്യൂരിറ്റി ഓഡിറ്റിംഗ് നടത്തുന്നതിനുള്ള താൽപര്യപത്രം"** എന്ന് രേഖപ്പെടുത്തേണ്ടതാണ്. നിശ്ചിത സമയ പരിധിക്കുള്ളിൽ ലഭിക്കാത്ത താൽപര്യപത്രം സ്വീകരിക്കുന്നതല്ല. മേൽസൂചിപ്പിച്ച താൽപര്യപത്രവുമായി ബന്ധപ്പെട്ട കൂടുതൽ വിവരങ്ങൾക്ക് അക്കൗണ്ട്സ് (ഡി) വിഭാഗവുമായി (0471-2512422) ബന്ധപ്പെടേണ്ടതാണ്.

പ്രീത കെ.,
അണ്ടർ സെക്രട്ടറി II (അക്കൗണ്ട്സ്).

Expression of Interest invited for the Security Audit of Web Application including Web services from CERT-In Empanelled Organizations

Scope of Work

Kerala Legislature Secretariat (KLS) is inviting Expression of Interest from CERT-In Empanelled Agencies for the Security audit of one Web application including Web Services. The said applications need to obtain the "safe-to-host" certificate from CERT-In empanelled agencies before hosting the same on State Data Centre.

Technical details of the applications are attached as **Annexure 1** for reference. The selected CERT-In empanelled security auditor should comply the following:

- The applications should be audited as per the CERT-IN Guidelines and other industry best practices.
- The applications should be thoroughly audited and must identity all the security vulnerabilities with the objective of enhancing the security of the applications.
- Provide recommendations to mitigate all identified risks and ensured that it is free of any known vulnerabilities or exploits.
- The Auditor should co-operate and provide all necessary details or evidences, as requested by KLS.
- The selected security auditor should provide continuous support to the development team in fixing of the vulnerabilities found during the security audit, if required.
- On successful completion of the security audit, furnish certificate for the applicaitons stating that the applications are safe for hosting on the SDC server.

Terms and Conditions

- Only those organisations/firms that are currently empanelled with CERT-In are eligible for submitting the Expression of Interest
- The security audit certificate must be in compliance with the CERT-In standards.
- The payment will be made only after submitting the final security audit certificate on completion of the Audit.
- No claim for interest in case of delayed payment will be entertained by the KLS.
- The time required to complete 'security audit' should be clearly mentioned in the Expression of Interest .
- Incomplete or conditional tender will not be entertained.

KERALA LEGISLATURE SECRETARIAT
THIRUVANANTHAPURAM

- The first round of Security Audit report should be submitted within 2 weeks after the work order is issued and consecutive round report if any, should be submitted within 15 working days.
- KLS can inspect/review the audit activities being undertaken by the auditor at any point of time.
- The required access to the website's, web applications will be provided to the selected CERT-In empanelled Security Auditor. The auditor should sign a Non-Disclosure Agreement with KLS.

Annexure - I

APPLICATION SECURITY AUDIT - SCOPING SHEET
Webcasting Application

S.No.	Web Application Assessment Details	Description
1	How many web application instance to assesses?	1 Web Application with thin client architecture.
2	How many login systems to assesses?	1 (Admin login)
3	How many static pages to assesses? (Approximate)	0
4	How many dynamic pages to assesses? (Approximate)	30-35 pages
5	Do you need fuzzing performed against this application?	Yes
6	Do you need want role-based testing performed against this application?	Yes
7	Do you need want credentialed scans of web applications performed?	Yes
8	Back-end Database(MS-SQL Server, PostgreSQL, Oracle, etc.)	PostgreSQL
9	Authorization No. of roles & types of privileges for the different roles	10
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	Yes, CMS portal utilizes Django to manage video files and their corresponding metadata.
11	Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) – PHP	Front-end Framework: React JS
12	Operating System Details(i.e.Windows-2003, Linux, AIX, Solaris, etc.)	Ubuntu 22.04
13	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Nginx
14	Total No. (Approximate) of Input Forms	20-25
15	Total No. of input field	60-70
16	Total No. of login modules	1