KERALA STATE AUIDT DEPARTMENT
DIRECTORATE, 4TH FLOOR ,VIKAS BHAVAN, PMG Jn
THIRUVANANTHAPURAM,KERALA-695033
Phone : 0471-2303640, email : directoritksad@gmail.com, director.ksad@kerala.gov.in
website : www.ksad.kerala.gov.in

No: DKSA/1152/2018/IT Cell2 Dated 31.08.2021

Proposals Invited

Sub : KSAD- Securtity Audit of Departmental software application-
- Proposal invited- Regarding

Ref : GO(MS) No.8/2019/ITD dated 22.04.2019

Kerala State Audit department are the statutory auditors of Local funds of the State of Kerala under the administrative control of Finance Department,Government of Kerala. The Director of the Department is also the Treasurer of Charitable Endowments of the State.The Department has automated the Charitable Endowments maintatined by the Director to be put to realtime use in the online platform. As per the protocol, the Departmental application has to be security audited by CERT empanelled agencies before hosting in the State owned State Data Center. Hence proposals are invited from the Cert empanelled agencies for conducting the security auidt of the application. The brief details of the application (Charitable Endowment Management System) is enclosed herewith for perusal

Interested agencies may forward the proposals or scoping sheets to directoritksad@gmail.com or director.ksad@kerala.gov.in or through post

Last date for the receipt of proposal : 15.09.2021

The proposals shall be evaluated by the Technical Committee of the Department comprising of Kerala State IT Mission and IIIT-M-Kerala Senior Consultants and their recommendation shall be final.

D. SANKY
Director of Kerala State Audit Department

Name of Web Application	Charitable Endowment Mangement System [CEMS]
Brief description of the Web Application	Charitable Endowments Management System is a digital platform for managing all the Endowment related activities like Endowment Request Processing, FD Management, Interest Management and Claim Distribution. The system has also got an automated Double Entry Accounting System which records all the Endowment related accounting transactions.
Web Application URL :	http://demo.kran.in:8081/Endowment/
No of web application instance to assesses	1
No of login systems to assesses	1
No of static pages to assesses (Approximate)	40
No dynamic pages to assesses (Approximate)	70
If fuzzing required against this application?	No
If role-based testing required against this application	No
If credentialed scans of web applications required	No
Back-end Database(MS-SQL Server, PostgreSQL, Oracle, etc.)	MySQL 5.7
Authorization No. of roles & types of privileges for the different roles	Public User - 2, Normal User - 2, Power User - 1
If the application contains any content management module (CMS	No
Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) – PHP	JSP, Jquery, XML
Operating System Details(i.e.Windows-2003, Linux, AIX, Solaris, etc.)	Linux
Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Apache Tomcat 7.0.96
Total No. (Approximate) of Input Forms	40
Total No. of input field	200
Total No. of login modules	1
Number of Web Services, if any	Nil
Number of methods in all web services	Nil
Number of URL's require to assesses	1
REST /SOAP based Application	No
Application security audited before	No

Director

Kerala State Audit Department

150 YEARS OF CELEBRATING THE MAHATMA

GOVERNMENT OF KERALA

Abstract

Electronics & Information Technology Department – Hosting of websites in State Data Centre after security auditing – Guidelines – Approved- orders issued

---

ELECTRONICS & INFORMATION TECHNOLOGY (C) DEPARTMENT

G.O (MS) No.8/2019/ITD Dated, Thiruvananthapuram,22.04.2019

Read:-1.GO(Rt) No.17/2011/ITD Dated:24.01.2011
2.GO(Ms)No.43/2015/ITD dated:01.10.2015
3.Letter No. CERT-K/11/2018-KSITM/278 from the Director, Kerala State IT Mission

ORDER

Government of Kerala has set up two State Data Centres (SDC1 & SDC2) to boost the e-governance activities in the State.Data centre enables various Government Departments/Statutory organizations to host their services or applications on a common infrastructure leading to ease of integration and efficient management. State Data Centre is one of the core infrastructure components to consolidate services, applications and infrastructure to provide proficient electronic delivery of G2G, G2C and G2B services. Likewise the Kerala State Wide Area Network (KSWAN), provides connectivity up to Taluk level offices and these entities notified as critical information Infrastructure of the state. In consonance with National Cyber Security Policy, 2013 both the State Data Centers have been ISO 27001 certified and periodic audits of the network infrastructure and co-hosted servers are performed quarterly by Third Party Security auditors, in addition to being subjected to STQC auditing annually. These measures will only ensure security of the cyber infrastructure but the security of the application software is not ensured through the above audits.

2. Currently both the data Centers host around 500 portals / websites / applications catering to the requirement of respective Government Departments/Organizations. These are either developed/managed by Total Solution Provider like NIC, KELTRON, C-DIT or developed and managed by third party companies like TCS, Wipro, Infosys etc and perhaps a few by home grown Startup companies. In addition to the web-based applications, Mobile applications (some standalone and some having a corresponding back-end console and reporting functionalities) are also getting developed for the state. In the applications so developed, there exists a possibility of cyber-attack due to flaws in the design, development and deployment of application. The vulnerabilities thus created may be exploited by intruders with malicious intent to cause defacements, data corruption, data/information leakage and disruption in service continuity, threat to data security and privacy.

3. In order to mitigate or minimize the cyber threats and to plug the vulnerabilities Government issued the following guidelines with regard to security auditing of websites and web and mobile based e-Governance applications:

I. Any e-Governance application to be hosted at the SDCs or elsewhere shall be security audited before launching in Production and mandates to obtain "Safe to host Certification" from a CERT-In empanelled Security Auditing agency before opening the application to the public. Security Audits and penetration testing are required to be performed followed by subsequent hardening aimed to mitigate the vulnerabilities and strengthening the security of the applications and their environment. As a policy, all websites / applications hosted at the State Data Centres have to go through a complete security audit process before they can be hosted or whenever an alteration/addition is made to the application. Periodic application security audits shall be done, at least once every two years.

II. The security audit / penetration testing is undertaken at various stages before, during and after hosting. Before hosting, Security audit of Web Application is done as per latest OWASP standard and report is submitted with vulnerabilities that require remediation. A second level testing for verification of whether all the discovered vulnerabilities are patched is also done before Issuance of Certificate of 'Safe to Host'' During hosting, Configuration review / SSL deployment, Random Penetration Testing of hosted application etc. also are done.

III. Application Security Audit covers some or all but not limited to the following activities:

- Identify the application level vulnerabilities on applications hosted in a test site / production site based on the latest top 10 OWASP vulnerabilities
- On demand application scans
- An audit of the environment along with the application to ascertain any vulnerability in the environment where the application is hosted.
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Web server information security
- Malicious File Uploads
- Provide recommendations for remediation of identified vulnerabilities. The report should contain discovered vulnerabilities and description of vulnerabilities and mitigation or remediation recommendations for fixing and patching of existing and found vulnerabilities as a part of solution.
- Follow a specific format for reports.
- Certify the applications / websites tested as "Safe for Hosting" and in times if Electronic Payment Gateway Operators request to provide it in their format.
- Accept responsibility for declaring the websites / URLs / mobile applications free from known vulnerabilities
- Any other activity concerning security audit related aspects; not essentially covered by work-areas outlined above.

4. Considering the requests received from various Government departments/Public Sector Undertakings/Organizations to address one of their concern that to engage a suitable agency for timely completion of security audits, and to rollout the e-governance applications in time, Government are pleased to empanel two CERT-IN empanelled home-grown startup companies M/s Value Mentor Consulting LLP and M/s Mirox Cyber Security & Technology Pvt Ltd, in line with G.O.(Rt)No.36/2018/SPD Dated 17/09/2018 issued for enabling the departments to procure products/services from Startup up companies directly without any tender procedure. The empanelment and the standardized rate card of Services rendered as agreed to by both the companies, enables the departments / organizations to select a security auditor to entrust the security auditing procedure. In addition to this, their services can also be utilized for preparation of Disaster Recovery and Business Continuity Plan formulations as well.

The empanelment is subject to the following rates, Conditions and guidelines.

Scope of work and deliverables

I. Security audit for Web or browser based application and Website

The selected vendor may cover the below mentioned tests for the application or website provided for testing:

1. Application Security Audit
2. Penetration Testing
3. Vulnerability Testing
4. Database Server Controls
5. Physical Access Control
6. Network security Review as part of Application Security
7. Compliance Review

Black box testing for Security Audit should follow OWASP guidelines covering to the testing below:

1. Cross-site scripting (XSS)
2. Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
3. Input Validation flaws
4. Malicious file execution
5. Insecure direct object references
6. Cross-site request forgery (CSRF)
7. Information leakage and improper error handling
8. Broken authentication and session management
9. Insecure cryptographic storage
10. Insecure communications
11. Failure to restrict URL access
12. Denial of Service

II. Scope of security audit for Desktop based application

1. Test user's rights and roles-authorized person should allow to login
2. Test security of data or information stored in application

3. Role based Security (Privilege Escalation)
4. Authentication Bypass or Unauthorized Access
5. Improper Error handling
6. Buffer Overflow
7. Denial of Services
8. Insecure Communications
9. Insecure Cryptographic Storage

5. Government are pleased to approve the following rates for security audits:

1. Websites/ Applications

TABLE 1.1 - Purely Static website (only informational content and no dynamic functionality)				
Sl No.	**Parameters of Organisation**	**Parameter range**	**Cost**	**Remark**
1	Static pages	Less than 20 pages	Rs.15000 fixed rate for the site audit	These rates will apply only if the website does not have any dynamic functionality at all and is purely static.
2	Static pages	More than 20 pages	Rs.25000 fixed rate for the site audit	

TABLE 1.2 - Dynamic website/ application BASIC SLAB DESCRIPTION				
Sl No.	**Parameters of Organisation**	**Parameter range**	**Cost**	**Remark**
1	Static pages	25 pages	Rs.25000 for audit of the site	Minimum Audit cost of a dynamic application is Rs.25000/-. If the application exceeds the threshold numbers in the basic slab, audit cost will be computed as: Rs.25000+ additional charges for static pages/ dynamic pages/ input forms, input fields, user roles exceeding the basic slab thresholds. Additional charge rates are given in Table 1.3.
2	Dynamics pages	3 pages extends upto 8 pages. If greater than 8, additional charges per page will apply.		
3	Input Forms	1 input form extend upto 3 forms. If greater than 3, additional charges per form will apply.		
4	Number of input fields	10 input fields extends upto 20 input fields. If greater than 20 input fields, additional charges per block of 10 input fields will apply.		
5	User Roles such as admin, manager, user	1 user role extends upto 2 user roles. If greater than 2, additional charges per user role will apply		

TABLE 1.3 - ADDITIONAL CHARGES for Dynamic website/ application in excess of BASIC SLAB			
Sl No.	**Parameters**	**Cost**	**Remark**
1	Static pages - per static page	Rs.400	These charges apply for the number of static pages/ dynamic pages/ input forms, input fields, user roles exceeding the basic slab thresholds given in Table 1.2.
2	Dynamics pages - per dynamic page	Rs.1000	
3	Input Forms - per form	Rs.2000	
4	Input fields - per block of 10 input fields	Rs.2000	
5	Per User Role such as admin, manager, user	Rs.3000	

2. **Android Mobile App**

TABLE 2.1 - Android Mobile App BASIC SLAB DESCRIPTION				
Sl No.	**Parameters of Organisation**	**Parameter range**	**Cost**	**Remark**
1	No of Screens in Android Mobile app	3 screens extends upto max 4 screens. If greater than 4, additional charges per screen will apply.	Rs.30000/- for audit of the Android Mobile App	Minimum Audit cost of an Android app is Rs.30000/-. If the app exceeds the threshold numbers in the basic slab, audit cost will be computed as: Rs.30000 + additional charges for screens/ input forms, input fields, user roles exceeding the basic slab thresholds. Additional charge rates are given in Table 2.2.
2	Input forms	2 input forms extends upto 3 forms. If greater than 3, additional charges per form will apply.		
3	Number of input fields	10 input fields extends upto 15 input fields. If greater than 15 input fields additional charges per block of 5 input fields will apply.		
4	User Roles such as admin, manager, user	1 max upto 2 User roles. If greater than 2, additional charges per user role will apply		

TABLE 2.2 - ADDITIONAL CHARGES for Android Mobile App in excess of BASIC SLAB			
Sl No.	**Parameters**	**Cost**	**Remark**
1	Per Screen in Android Mob app	Rs.1000	These charges apply for the number of Screens/ input forms, input fields, user roles exceeding the basic slab thresholds given in Table 2.1.
2	Per Input forms	Rs.2000	
3	Per block of 5 input fields	Rs.5000	
4	Per User Role such as admin, manager, user	Rs.3500	

3. **iOS Mobile App**

TABLE 3.1 - iOS Mobile App BASIC SLAB DESCRIPTION				
Sl No.	**Parameters of Organisation**	**Parameter range**	**Cost**	**Remark**
1	No of Screens in iOS Mobile app	3 screens extends upto max 4 screens. If greater than 4, additional charges per screen will apply.	Rs.40000 for audit of the iOS mobile app	Minimum Audit cost of an iOS app is Rs.40000/-. If the app exceeds the threshold numbers in the basic slab, audit cost will be computed as: Rs.40000 + additional charges for screens/ input forms, input fields, user roles exceeding the basic slab thresholds. Additional charge rates are given in Table 3.2.
2	Input forms	2 input forms extends upto 3 forms. If greater 3, additional charges per form will apply.		
3	Number of input fields	10 input fields extends upto 15 input fields. If greater than 15 input fields, additional charges per block of 5 input fields will apply.		
4	User Roles such as admin, manager, user	1 max upto 2 User roles. If greater than 2, additional charges per user role will apply		

TABLE 3.2 - ADDITIONAL CHARGES for iOS Mobile App in excess of BASIC SLAB			
Sl No.	**Parameters**	**Cost**	**Remark**
1	Per Screen in iOS Mob app	Rs.2000	These charges apply for the number of Screens/ input forms, input fields, user roles exceeding the basic slab thresholds given in Table 3.1.
2	Per Input form	Rs.3000	
3	Per block of 5 input fields	Rs.7500	
4	Per User Role such as admin, manager, user	Rs.7500	

4. **Web Services**

TABLE 4 - Web Services			
Sl No.	**Parameters**	**Cost**	**Remark**
1	Web services / API - Per Server/IP	Rs.1,20,000 (if done remotely) + 30% extra (if done onsite)	

6. **Terms and conditions for compliance by the vendors**

The following terms and conditions for compliance by the approved vendors.

1. For security auditing of Government assets, the vendor shall not charge cost exceeding the rates finalized by the Government.

2. GST may be charged on top of cost arrived by applying the Rate Contract.
3. For any audit engagement, the vendor shall conduct a pre-assessment to understand the audit requirements of the organization/Department and shall provide the draft scope of work in detail at free of .cost, if requested by the organization.
4. The vendor shall provide the first audit report to the GoK organisation not later than 3 weeks from receiving the work order. Subsequent interim reports shall be issued not later than 8 working days of receiving the patched application for re-test.
5. For any audit engagement, besides the original first audit, the vendor shall do any number of re-tests at no additional cost till all issues are cleared by the user department within 90 working days of providing the first audit report. It should also ensure no new vulnerabilities are introduced as part of code changes to fix the reported vulnerabilities.
6. The vendor may be terminated from audit engagements for reasons such as dishonouring audit commitments or violating these terms and conditions, degradation of auditor's performance or competence to meet expectations or if empanelment at CERT-India ceases.
7. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.
8. For any audit engagement, the vendor shall provide support to the auditee technical team in fixing the security issues reported in first audit or any subsequent audit in terms of handholding and training. The support should include a minimum of 1 day onsite or remote training or handholding on how to fix the issues.
9. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.
10. The vendor shall not sub contract any part of work assigned to another vendor or engage non-employees to perform the work.
11. A formal Confidentiality & Non-Disclosure Agreement should be signed by the vendor to keep confidential all the information that it has access to during the course of its actions. Employees at the vendor organization should sign individual NDAs. As per CERT-In advisory, the empanelled vendor must ensure that data collected during audit work and reports prepared are not taken out of the auditee organization's premises/ network and/ or shared to anyone except the auditors, auditee organization, CERT-In and any other authorized Government entity. Any audit data should be wiped out from the vendor's domain after any engagement.
12. In the case of Application Vulnerability Assessment/ Penetration Testing (VAPT), the Auditor will be required to audit and test the website on the staging server/testing environment provided by hosting service provider before issuing the audit certificate.
13. The vendor shall provide any audit report or data as required by KSITM with respect to audits performed for Government of Kerala.

7. **Process of procurement of auditing services from approved vendors**

1. A Government Department/Organisation can directly procure websites/Mobile applications security audit from any of the Government approved vendors at the proposed rates.
2. For software applications and security audit including penetration test for networks, the Departments/Agencies shall go for limited tenders from the CERT-In empaneled agencies based in Kerala or use the services of STQC.
3. In order to ease the scoping exercise, the auditee organization shall request any one of the approved vendor to help in scoping its audit work. The vendor should ensure the auditee organization is absolutely clear about the scope of work.
4. If the scope of audit includes any other work other than Application/ Web Service/ Mobile App/ Server/ Network Security Audit (example, ISO27001 audit, PCI DSS audit etc), the Goverment Department/Organization shall follow Government tender procedures to award work to the L1 bidder among the approved vendors.
5. As part of any audit engagement, the approved vendors may submit detailed proposals including:
    1. Details of different tests/ audits to be performed, standards against which the audits will be performed etc.
    2. Details to include specific systems/ subsystems to be audited and what activities will be performed in the subsystems.
    3. Clear component-wise cost estimate including :
        - Manpower rate and effort estimate in number of man-days, if Security audit includes items other than Application/ Web service/ Mobile App/ Server/ Network Security Audit.
        - Schedule for completion of the work.
6. Application security audit cost is impacted by the correctness of parameters such as Number of Static/ Dynamic Pages, Number of Input Forms, Number of input data fields, Number of user roles etc. These should be recorded by the department through the Development team in scoping sheet and provided to the vendor. The vendor may be provided test user credentials (if applicable) on the application on test server in order to corroborate the same. Any discrepancies between the developer provided data and vendor provided data may be mutually sorted out before reaching an agreement on the scope and further submission of cost proposal by the vendor. Subsequently, the department needs to revoke the password provided to the vendor until work is awarded.
7. Upto 25% of the amount fixed may be paid as mobilisation advance. 50% payment of the charges may be paid to the vendor on submission of the first Audit report. Balance 25% will be released only after issue of the final audit report and Security Audit Certificate.
8. In case of Application security audits, the auditee organization should ensure that the reported issues are fixed and resubmitted for the re-audit within no more than 3 weeks of the issue of the first audit report. On subsequent cycles, the organization should fix issues given in interim report within 2 weeks of the issue of interim report. In any event, the whole process of starting the audit by the

vendor till issues of the final audit certificate should be completed within 2 months.

9. Any complaints about the auditing vendor shall be communicated to the Director, KSITM.
10. The Government Department/Organization shall formally request any of the approved vendors to do a pre-assessment of its Information Systems, if such requirement exists. The vendor shall do a pre-assessment at free of cost to understand what information systems are used by the organization and advise the organization on scope of security auditing from a risk perspective. The auditee organization may take a decision on scoping the information systems audit. The Department/Organization shall consult Kerala State IT Mission for any advice in the matter.
11. The Department/Organization shall send a copy of the work order to the Director, Kerala State IT Mission.
12. The above guidelines would apply for all cases where limited tenders are floated.

(By Order of the Governor)

M.SIVASANKAR
SECRETARY

To

The Director, Kerala State IT Mission, Thiruvanthapuram
The Registrar, High Court of Kerala, Ernakulam (with C/L)
The Secretary, Kerala Public Service Commission, Thiruvanthapuram (with C/L)
The Director General of Police, Thiruvanthapuram
The Advocate General, Ernakulam
All Departments in Secretariat (including Law and Finance)
All Heads of Departments (Through administrative Departments)
Chief Executive Officer/Managing Director of All PSUs/Autonomous Bodies (Through Administrative Departments)
All District Collectors
The Registrar, All Universities in Kerala
M/S Value Mentor Consulting LLP, Infopark, Thrissur
M/S Mirox Cyber Security & Technology Pvt Ltd, Technopark, Thiruvanthapuram } (Through KSITM)
The Account General (A &E), Kerala, Thiruvanthapuram
Stock File/Office Copy

Forwarded/ By Order

Section Officer