ANNEXURE – I

APPLICATION DETAILS & SCOPE OF WORK FOR SECURITY AUDIT

1. APPLICATION TECHNICAL PROFILE & SCOPING DETAILS

The following parameters define the technical architecture, application environment and boundary conditions of the web application proposed to be audited. Bidders shall base their technical and financial proposals on the specifications and scope indicated below.

A. General & Administrative Parameters

Sl. No.	Parameter	Details
1	Application Name & Description	SOIL DMS (Document Management System)
2	Application Developer	Keltron (Kerala State Electronics Development Corporation Ltd.)
3	Client Department	Department of Soil Survey and Soil Conservation, Government of Kerala
4	Application URL	10.5.95.55/soilsurvey/staff_login_doc.php
5	Testing Environment	Staging / Local Network (LAN)

B. Technical Specifications & Complexity Matrix

Sl. No.	Assessment Parameter	Details / Count
1	Web Application Instances to be Assessed	1
2	Total URLs to be Assessed	1
3	Total Login Systems to be Assessed	1
4	Number of User Roles & Types of Privileges	3
5	Static Pages to be Assessed	Approximately 0
6	Dynamic Pages to be Assessed	Approximately 30
7	Total Input Forms	5
8	Total Input Fields	Approximately 30
9	Total Login Modules	1
10	Front-end Tool / Server-side Scripts	PHP
11	Back-end Database	PostgreSQL
12	Operating System	Ubuntu 22.04
13	Web / Application Server	Apache 2.4
14	Content Management System (CMS)	None
15	Web Services / APIs	Not Applicable (N/A)
16	Fuzzing Required	Yes

17	Role-based Testing Required	Yes
18	Credentialed Scans Required	Yes, wherever technically feasible

2. SCOPE OF WORK & VULNERABILITY ASSESSMENT

The selected CERT-In empanelled auditor shall conduct a comprehensive Security Audit comprising Vulnerability Assessment and Penetration Testing (VAPT) of the SOIL DMS web application.
The system shall be comprehensively audited, within the approved scope of work, to identify known and reasonably discoverable security vulnerabilities using appropriate industry-standard methodologies, tools and manual testing techniques, with the objective of strengthening the overall security posture of the system.

2.1 Compliance & Applicable Standards

The audit shall be conducted in accordance with the latest applicable CERT-In guidelines, directions and audit requirements, including the CERT-In Comprehensive Cyber Security Audit Policy Guidelines and applicable guidelines for secure application design, development, implementation and operations, as amended from time to time. Reference frameworks include:

a) OWASP Top 10 Web Application Security Risks;
b) OWASP Web Security Testing Guide (WSTG);
c) OWASP Application Security Verification Standard (ASVS);
d) Common Weakness Enumeration (CWE);
e) Common Vulnerability Scoring System (CVSS); and
f) Applicable CERT-In advisories, directions, and Kerala State Data Centre guidelines.

2.2 Key Audit Objectives

The audit shall, at a minimum, seek to identify and assess:

a) Security vulnerabilities and weaknesses in the application;
b) Authentication and session-management weaknesses;
c) Authorization and access-control weaknesses;
d) Injection vulnerabilities;
e) Cross-site scripting vulnerabilities;
f) File upload and document-management vulnerabilities;
g) Information disclosure;
h) Server and database misconfigurations;
i) Business logic and workflow weaknesses;
j) Vulnerabilities that may lead to unauthorized access or disclosure of documents; and
k) Other vulnerabilities identified during the course of the assessment within the

approved scope.

2.3 Technical Testing Requirements

2.3.1 Input Handling & Data Validation

The auditor shall assess the identified dynamic pages, input forms and input fields for improper input validation and sanitization.

The assessment shall include, but not be limited to:

i. SQL Injection, including PostgreSQL-specific injection techniques;
ii. Operating System Command Injection;
iii. Code Execution vulnerabilities;
iv. Cross-Site Scripting (XSS), including Stored, Reflected and DOM-based XSS, wherever applicable;
v. Input validation bypass;
vi. Manipulation of request parameters, hidden fields and cookies;
vii. Improper handling of special characters and unexpected input; and
viii. Validation of all identified input forms and input fields.

2.3.2 Authentication & Session Management

The auditor shall assess:

i. Secure login handling;
ii. Session timeout mechanisms;
iii. Cookie security attributes including HttpOnly, Secure and SameSite, wherever applicable;
iv. Password policy and password handling;
v. Brute-force vulnerabilities;
vi. Credential exposure;
vii. Session fixation;
viii. Session token security;
ix. Session hijacking vulnerabilities;
x. Secure logout and session invalidation; and
xi. Other weaknesses in authentication and session management.

2.3.3 Authorization & Access Control

The auditor shall assess:

i. Insecure Direct Object References (IDOR);
ii. Unauthorized access to documents, files and internal pages;
iii. Horizontal privilege escalation;
iv. Vertical privilege escalation;
v. Forced browsing;
vi. Access-control bypass;

vii. URL and parameter manipulation; and
viii. Access restrictions applicable to the identified user roles.

2.3.4 File Upload Security

Since the application functions as a Document Management System, all file/document upload functionality shall be subjected to detailed security assessment.

The assessment shall include, but not be limited to:

i. Validation of permitted file extensions and file types;
ii. MIME type validation and verification of actual file content;
iii. Testing for bypass of file-type restrictions;
iv. Double-extension and specially crafted file-name testing;
v. Testing for malicious file uploads;
vi. Testing for executable file and web-shell upload, wherever technically applicable;
vii. Directory traversal through file names, parameters or upload requests;
viii. Unauthorized file overwrite, replacement or modification;
ix. File-size restrictions and potential resource-exhaustion vulnerabilities;
x. Verification that uploaded files are stored in a secure location;
xi. Verification that uploaded files cannot be directly executed through the web server;
xii. Verification that uploaded documents cannot be accessed without appropriate authentication and authorization;
xiii. Testing for unauthorized access to documents belonging to other users or roles;
xiv. Testing for manipulation of uploaded file references and parameters;
xv. Testing of specially crafted documents that may result in unauthorized code execution or information disclosure; and
xvi. Verification of appropriate security controls for uploaded files before they are made available for access or download.

2.3.5 Server & Infrastructure Hardening

The audit shall include review of relevant Apache Web Server and Ubuntu operating system configurations within the approved scope.

The assessment shall include:

i. Apache web-server configuration;
ii. Server banner and version disclosure;
iii. Directory browsing/listing;
iv. Unnecessary HTTP methods;
v. TLS/SSL configuration;
vi. Weak protocols or cipher suites, wherever applicable;
vii. Security-related HTTP response headers;
viii. System-level information disclosure;
ix. Custom error-page configuration;
x. Default or unnecessary services/configurations; and
xi. Other security misconfigurations identified during the assessment.

2.3.6 PostgreSQL Database Security

The auditor shall assess relevant PostgreSQL database security configurations, including:

i. Database access controls;
ii. User accounts and privileges;
iii. Least-privilege implementation;
iv. Database configuration relevant to application security;
v. SQL Injection-related database access;
vi. Database error handling and information disclosure;
vii. Excessive or unnecessary database privileges;
viii. Exposure of database credentials or configuration information; and
ix. Security of sensitive information handled by the database.

2.3.7 Logic & Error Handling

The auditor shall assess:
i. Business logic bypass;
ii. Unauthorized manipulation of document-management workflows;
iii. Improper error handling;
iv. Disclosure of server paths;
v. Disclosure of database structure;
vi. Disclosure of PHP code or application configuration;
vii. Stack traces and technical error information; and
viii. Other application logic weaknesses.

2.3.8 Fuzzing and Automated Vulnerability Assessment

The auditor shall conduct appropriate automated vulnerability scanning and fuzzing of the application.

Testing shall include, wherever applicable:

i. Input fields;
ii. URL parameters;
iii. HTTP request parameters;
iv. File upload functionality;
v. Application endpoints; and
vi. Other identified attack surfaces.

Automated findings shall be appropriately validated before being reported as confirmed vulnerabilities, wherever technically feasible.

2.3.9 Role-Based Testing

Role-based testing shall be carried out for the identified user roles to verify:

i. Access to authorized pages and functions;

ii. Access to authorized documents and records;
iii. Ability to modify or delete information;
iv. Administrative access restrictions; and
v. Horizontal and vertical privilege escalation.

2.3.10 Credentialed Security Assessment

Where appropriate credentials are made available, the auditor shall perform authenticated/credentialed security testing to identify vulnerabilities that may not be detectable through unauthenticated testing.

3. VULNERABILITY CLASSIFICATION

Vulnerabilities shall be classified by severity: Critical, High, Medium, Low, and Informational, with CVSS ratings and OWASP/CWE mappings. Each finding shall detail:
a) Vulnerability Description & Affected Component/URL/module
b) Security/Business Impact
c) Proof-of-Concept & Supporting Evidence
d) Severity/risk rating
e) Recommended Remediation & Priority

4. SUPPORT FOR REMEDIATION, RE-TESTING AND DELIVERABLES

The selected security auditor shall provide necessary technical clarification and recommendations to the Department/KELTRON technical team for remediation of vulnerabilities identified during the audit. The auditor shall subsequently conduct follow-up/verification testing to confirm the closure of such vulnerabilities.

Deliverables include:

4.1. Initial VAPT Audit Report: The report shall contain, at a minimum:

a) Executive summary of the security posture;
b) Scope and limitations of the assessment;
c) Audit methodology;
d) Standards/frameworks followed;
e) Tools and techniques used;
f) Detailed vulnerability findings;
g) Severity classification;
h) CVSS rating, wherever applicable;
i) OWASP/CWE mapping, wherever applicable;
j) Affected URL, module, parameter or component;
k) Description of each vulnerability;
l) Security/business impact;
m) Proof-of-Concept steps;

n) Screenshots or other supporting evidence, wherever applicable;
o) Specific remediation recommendations; and
p) Recommended remediation priority.

4.2. Vulnerability Summary Matrix: The auditor shall provide a consolidated vulnerability summary in the following format:

Sl. No.	Vulnerability	Severity	Affected Component	CVSS	Remediation Priority	Status
1						
2						
3						

4.3. Re-testing & Verification Report: After remediation of the reported vulnerabilities, the auditor shall conduct re-testing and submit a report clearly indicating:

a) Vulnerabilities successfully closed;
b) Vulnerabilities partially remediated;
c) Vulnerabilities remaining open; and
d) Any new vulnerabilities identified during re-testing.

4.4. Final Security Audit Report & Certificate: The final security audit report and certificate shall conform to the applicable CERT-In requirements and Kerala State Data Centre guidelines.

4.5. Safe-to-Host Certificate: Issued upon satisfactory remediation/closure or formal acceptance of vulnerabilities in accordance with CERT-In/Kerala State Data Centre requirements.

5. AUDIT, REMEDIATION AND RE-TEST TIMELINE

The audit shall be completed within 15 working days from the date of provision of all required access, information and test environment. The Auditor shall submit the initial audit report within 3 working days of completion of testing. Follow-up verification shall be conducted after remediation of the identified vulnerabilities.

Indicative Timeline Breakdown:

Sl. No.	Activity	Timeline
1	Kick-off and information gathering	Within 2 working days from commencement
2	Vulnerability Assessment and Penetration Testing	Within 7 working days thereafter
3	Submission of Initial VAPT	Within 3 working days after completion of

	Report	testing
4	Re-testing after remediation	Within 5 working days of intimation regarding completion of remediation
5	Submission of Final Report and Safe-to-Host Certificate	Within 3 working days after completion of re-testing

Any delay arising from non-availability of application access, credentials, or required technical support from the developer shall not be attributable to the auditor.

6. CONFIDENTIALITY AND SECURITY OF AUDIT DATA

All credentials, logs, source code, configuration details, audit artefacts, reports and other information accessed or generated during the audit shall be treated as confidential and shall be stored, transmitted and handled securely in accordance with applicable CERT-In requirements and the directions of the Department/Kerala State Data Centre. No such information shall be disclosed to any third party without prior written approval of the Department, except where disclosure is required under applicable law or CERT-In requirements.

7. AUDIT CONDUCT & ACCEPTANCE

• The audit must be conducted safely to avoid service disruption or data loss. Destructive testing or DoS testing is strictly prohibited unless specifically authorized in writing.
• The audit shall be considered officially completed only upon submission of the final security audit report and 'Safe to Host' certificate, duly accepted by the Department and Kerala State Data Centre.

Digitally signed by
Saju K. Surendran
Date: 31-08-2026
11:51:41

SAJU K SURENDRAN IES

DIRECTOR
Department of Soil Survey and Soil Conservation