

**DEPARTMENT OF SOIL SURVEY & SOIL CONSERVATION****Directorate HQ**

Vazhuthacaud, Thiruvananthapuram

email: soildirector@gmail.com; Phone: 0471-2778760/1

No:SSSC/1182/2026-PG3

Date:29-09-2026

ANNEXURE - I**SCOPE OF WORK FOR SECURITY AUDIT****1. TECHNICAL PROFILE**

The technical architecture of the items proposed to be audited is shown below.

Sl. No.	Item	IP Address/Type
1	Virtual Machine1	10.5.41.90
2	Virtual Machine2	10.5.41.91
3	Virtual Machine3	10.5.41.92
4	WebGIS Application	ArcGIS Enterprise Professional Plus

2. SCOPE OF WORK & VULNERABILITY ASSESSMENT

The audit will cover the internal collaborative WebGIS workspace, public-facing services, underlying operating systems, spatial databases and application-level controls.

2.1. INFRASTRUCTURE & VM CONFIGURATION SECURITY

2.1.1. Operating System (OS) Hardening: Security evaluation of the OS installed on all three (3) VMs against standard security benchmarks (e.g., CIS benchmarks), checking for unpatched vulnerabilities, missing security updates and unnecessary background services.

2.1.2. Network & Firewall Rules: Audit of network configuration, IP filtering, subnet isolation, and firewall policies governing traffic flow to/from the SDC environment.

2.1.3. Port & Service Management: Identification and evaluation of open ports, running protocols, and active services across all three VMs to ensure only required ports are exposed.

2.2. ARCGIS ENTERPRISE & WEBGIS APPLICATION SECURITY

2.2.1. ArcGIS Component Security: Auditing the security posture of installed ArcGIS Enterprise components (ArcGIS Server, Portal for ArcGIS, ArcGIS Data Store and ArcGIS Web Adaptor).

2.2.2. Web Application & API Security: Penetration testing of custom/default web applications, WebGIS portals and published RESTful APIs. Testing must align with OWASP Top 10 standards, Applicable CERT-In Advisories and KSDC guidelines.

2.2.3. Public-Facing WebGIS Hardening: Security assessment of public services to prevent data leakage, unauthorized parameter tampering, or service denial via public map services, feature layers, and basemaps.

2.3. AUTHENTICATION, AUTHORIZATION & PRIVILEGE MANAGEMENT

2.3.1. User Authentication: Assessment of identity management, password policies, session management, and multi-factor authentication (MFA) mechanisms for departmental users across the State.

2.3.2. Role-Based Access Control (RBAC): Verification of privilege separation—ensuring authorized users have access only to assigned spatial data, layers and attributes.

2.3.3. Editing & Admin Privilege Controls: Testing access controls to ensure strict boundary isolation between:

- (i) Departmental editors (data creation, modification, and updating).
- (ii) Data validators and approvers.
- (iii) General public users (view-only access to published outputs).

2.4. DATABASE & SPATIAL DATA SECURITY

2.4.1. Enterprise Geodatabase Security: Security review of the enterprise spatial database management system hosted within the VM infrastructure.

2.4.2. Data Access Restrictions: Verification that internal editable spatial datasets are isolated and cannot be accessed, modified, or extracted directly through public-facing endpoints.

2.4.3. Data Transmission & Storage: Evaluation of encryption standards applied to data-at-rest (geodatabase/VM storage) and data-in-transit (SSL/TLS protocols between users, servers and SDC).

2.5. VULNERABILITY ASSESSMENT & CONTROLLED PENETRATION TESTING (VAPT)

2.5.1. Internal VAPT: Simulated attacks from the perspective of an internal user to check for lateral movement, privilege escalation and unauthorized access to unapproved or restricted spatial layers.

2.5.2. External (Public-Facing) VAPT: External black-box/grey-box penetration testing targeting the public WebGIS interface to test resilience against web attacks, data extraction attempts and unauthorized endpoint discovery.

2.5.3. Remediation Verification (Re-Audit): Conducting a follow-up assessment post-remediation to verify that all identified vulnerabilities have been properly patched.

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/KSDC 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:

(i) Detailed VAPT Report: Exhaustive list of discovered vulnerabilities categorized by severity (Critical, High, Medium, Low, Informational) with Proof-of-Concept (PoC) references.

(ii) Remediation Guidance Plan: Step-by-step recommendations for patching identified OS, ArcGIS, network, and application vulnerabilities.

(iii) 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.

(iv) Executive Summary Report: High-level summary of the overall security posture suitable for management and compliance requirements.

(v) Final Security Audit Report: The final security audit report shall conform to the applicable CERT-In requirements and KSDC guidelines.

(vi) Safe-to-Host Certificate: Compliance certification issued after successful re-testing and verification that all critical/high security gaps are closed. Issued upon satisfactory remediation/closure or formal acceptance of vulnerabilities in accordance with CERT-In/KSDC 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 Report	Within 3 working days after completion of 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 KSDC 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/KSDC. 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

7.1 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.

7.2. 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 KSDC.

Digitally signed by
Dathan C S
Date: 29-09-2026
12:10:12

Additional Director Soil Survey
ADDITIONAL DIRECTOR OF SOIL SURVEY