



**ANDHRA PRADESH TECHNOLOGY SERVICES LIMITED**  
(Government of AP Undertaking)  
(CERT-In Empanelled and ISO 9001:2015, ISO 27001:2013 Certified)  
3rd Floor, R&B Building, Opp. Indira Gandhi Municipal Stadium,  
MG Road, Labbipet, Vijayawada-520010, Andhra Pradesh, India.  
Ph.0866-2468108 | md\_apt@ap.gov.in | <https://www.apt.gov.in/>

## Security Certificate

(Unique Ref No: APTS/APCSP/Assurance/170/2025)

**Audit Performed by:** Andhra Pradesh Technology Services Ltd.

**Application Description/Name:** APTMS

**Staging URL of the web application:** <https://uat.aptms.in>

**Hash Value (SHA-512):**

3392d72ca968825970202786249bb3c3deef1cbf9d3a4dc8a7c3778ed7b93fa4bc9  
2ebf741c54a99634894e7414a7f5a7c7d79077d9dbc5d88131ea4cde1f67e

**Production URL of the web application:** <https://endowmentsinfo.ap.gov.in/>

**Application Type:** Dynamic

**Tested Roles:** Admin

**Audit Performed by:**

- **Name** : APTS Security Team
- **Email** : mgr-apcsp-apt@ap.gov.in
- **Telephone** : 9440469194

**Level -1 Audit date** : **06-10-2025**

**Level -2 Audit date** : **07-10-2025**

**Issue Date** : **07-10-2025**

**Unique Reference No.** : APTS/APCSP/Assurance/170/2025

The security audit for the APTMS Web Application of the Revenue Department, has been completed on a staging server with the <https://uat.aptms.in>. During the initial audit of the web application the following vulnerabilities were identified which have been successfully fixed by the development team:

- 1.Rate Limit Bypass**
- 2.Client Side Bypass / Improper Server Side Validation**
- 3.Browser Cache Weakness**
- 4.Version Disclosure**
- 5.Improper Input Validation**

### Conclusion:

APTMS Web Application was initiated on 03-10-2025 on staging server URL: <https://uat.aptms.in> by Andhra Pradesh Technology Services Ltd. The

initial and follow-up audits were done on the above-mentioned dates and there is no pending nonconformity w.r.t OWASP Top 10 (2024), SANS Top 25, Open Source Security Testing Methodology Manual (OSSTMM3) as on 07-10-2025.

APTMS Web Application meets all the aspects of Open Web Application Security Project (OWASP) Top 10 (2024), SANS Top 25, Open Source Security Testing Methodology Manual (OSSTMM3) and is safe for hosting provided the recommendations are implemented. APTMS Web Application of the Revenue Department in a secure opening environment will create an overall system that is resilient to known patterns of attack.

It is therefore our opinion that a typical user would require a sophisticated level of security attack skill to breach such a system. In this capacity, we are pleased to provide a positive rating on the security posture of APTMS Web Application of the Revenue Department. This application is free from any known vulnerabilities as on 07-10-2025.

The APTMS web application is free from all the known vulnerabilities as on date and is safe for hosting provided the recommendations are implemented.

**Recommendation:**

- All SSL/TLS related issues can be addressed on the production server
- All the above reported issues can be addressed on the production server
- All the test data should be removed before hosting on live environment.
- The entire application should be hosted with read only permission.
- Application should be reviewed before any major update is released.
- Patching of infrastructure and application must be done on regular basis.
- Admin login should be accessible through VPN only.
- The application which is tested by the team should have application version number.
- Do not use default / guessable credentials / test credentials in production environment.
- This certificate is valid till no modifications are done in the APTMS Web Application of the Revenue Department or six months from the date of issue whichever is earliest.

Date: 08-10-2025  
Place: Vijayawada

M. Krishnaveni  
Manager-IS Audit  
Andhra Pradesh Technology Services Ltd