|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/4/2018) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** AP State – GAD Web Application.  **Staging URL** :  **Production URL** of the web application: https://gad.ap.gov.in  **Audit Performed by:**   1. **Name :** Guthula Yaswanth Kumar 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 09-OCT-2018  **Level -02 Assessment date :** 23-OCT-2018  **Issue Date :** 23.10.2018  **Unique Reference No. :** APTS/APCSP/Assurance/4/2018  AP State- GAD Web Application, auditing is completed on a production server with URL/IP: https://gad.ap.gov.in. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Autocomplete – OFF 2. Login Brute Force 3. Version Disclosure 4. Potentially Vulnerable Headers 5. Internal IP disclosed     **CONCLUSION:**  Auditing for AP State – GAD Web Application was done on October 11.10.2018 in the production server URL: https://gad.ap.gov.in by Andhra Pradesh Technology Services Ltd. The follow-up audit was done on 22.10.2018 and there is no pending nonconformity w.r.t OWASP Top 10, 2017 as on 23.10.2018.  AP State – GAD Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. AP State – GAD Web Application 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 AP State – GAD Web Application. This application is free from any known vulnerabilities as on 23.10.2018.  The web application is free from all the vulnerabilities and is safe for hosting provided the recommendations are implemented.  **Recommendation:**   1. The entire application should be hosted with read only permission. 2. The application has to be tested quarterly for any vulnerability. 3. Application should be reviewed before any major update is released. 4. Patching of infrastructure and application has to be done on regular basis. 5. Admin login should be accessible through VPN only. 6. This certificate is valid till no modification in AP Sate – GAD Web Application is done or one year from the date of issue whichever is earlier.   Dr.G. Jacob Victor Date: 23.10.2018  Executive Director  For Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |