

**GOVERNMENT OF ANDHRA PRADESH
ABSTRACT**

IT,E&C Department – Andhra Pradesh Cyber Security Policy (APCSP) 2017 – Cyber Assurance Services by Nodal Agency – Critical Information Infrastructure to undergo Mandatory Audits by all Secretariat Departments/ HoDs/ PSUs/ Societies and Institutions – Orders – Issued.

INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS (INFRA)
DEPARTMENT

G.O.MS.No.4

**Dated:10.01.2019
Read the following:**

1. “National Cyber Security Policy in 2013”, notified in the Gazette of India Extraordinary No. 143, dated 02.07.2013.
2. G.O.MS.No.2, IT,E&C (Infra) Department, Dated.01.03.2017.
3. eOffice NF No.APTS/CS/CyberSOC/04/2017.

ORDER:

The Government of India had notified the “National Cyber Security Policy in 2013”. The National Policy lays down a number of strategies for realizing the vision of ‘building a secure and resilient cyberspace for citizens, businesses and Government’. The State of Andhra Pradesh has been a pioneer in the use of ICTs extensively for delivery of public services and felt the need to establish “Andhra Pradesh Cyber Security Policy”, to complement and supplement the National Cyber Security Policy 2013, and issued “Andhra Pradesh Cyber Security Policy 2017”, vide G.O 2nd read above.

2. Further, The IT,E&C Department has identified the M/s APTS Ltd. as a Nodal Agency on behalf of IT,E&C Department for implementing the APCSP. The objective of Cyber Security Policy (CSP) is to understand, address and manage the cyber security risks and improve management of Cyber Security in a cost-effective manner.

3. APCSP is applicable to all Government Departments and State owned entities and emphasises consistent approach for sustainable and effective cyber security implementation through Cyber Security Assurance Services.

4. The Cyber Security Assurance Services consist of security assessment of Department, Process Audit, VAPT (Vulnerability Assessment and Penetration Testing), Application Test and the Infrastructure Assessment as the case maybe.

5. All Departments should take the ownership of securing the Critical Information Infrastructure (CII), (IT infrastructure, Websites, Web and Mobile applications, etc.). The details of CII should be entered into the website created by APTS ([URL:https://ITAssets.aps.gov.in](https://ITAssets.aps.gov.in)).

6. All Departments should nominate an officer as a Single Point of Contact (SPoC), who shall be responsible for Security Compliance of respective Department and communicate with APTS/ APCSOC. In the absence of Primary SPoC, the details of the in-charge SPoC

should be entered in the Portal. The following are the responsibilities of the SPoC to ensure mandatory audits on CII:

- (a) Department SPoC shall identify the Non-active IT assets (Websites and Applications, Servers, etc which are not in use) and shutdown or disconnect them from internet to avoid attacks.
- (b) The Department SPoC will be provided access to the [URL:https://ITAssets.apt.gov.in](https://ITAssets.apt.gov.in) to enter CII details. All active IT assets shall be entered in to the portal by the SPoC.
- (c) The SPoC should ensure that CII shall undergo security audits mandatorily. SPoC should classify the IT asset as Critical/Medium/Low and schedule the security audits based on criticality as below:
 - (i). High Critical IT Assets - once in 3 months
 - (ii). Medium Critical IT Assets - once in 6 months
 - (iii). Low Critical IT Assets - once in a yearAPTS shall schedule and conduct the audits accordingly.
- (d) The process of Audit Compliance:
 - (i). APTS shall conduct the first level audit of the CII as provided by SPoC.
 - (ii). The identified findings during the audit will be made available to SPoC.
 - (iii). SPoC shall arrange for fixing (closing) the findings and update the closure status of the same on portal.
 - (iv). APTS shall confirm the closure of findings through follow-up (re-verification) audit.
 - (v). Steps ii, iii and iv shall be repeated until all the findings are closed and upon closure of all findings APTS shall provide Security Audit Compliance Certificate.
- (e) SPoC shall provision all assurance audit requirements such as relevant documentation, staging environment and access credentials to APTS as and when asked for conducting the Security Audit.
- (f) The Departments using the Third Party (SI, developer, etc.) services shall direct their service providers to provide the relevant documentation, staging environment and access credentials to APTS. It shall be the responsibility of Third party to close all the findings reported by APTS and report back to APTS through SPoC. The critical & high category findings shall be closed in 2 weeks and all the remaining findings shall be closed in 3 weeks from the date of audit report by the Third Party.
- (g) Failure to cooperate with APTS for auditing or delay in achieving the compliance beyond the time lines specified, the third party will be black listed for a period of 3-5 years from undertaking any work in Government of Andhra Pradesh.

7. The Security Audit Compliance Certificate issued by M/s APTS Ltd. shall be treated as equivalent to the one issued by CERT-In empanelled Third Party auditing agencies for hosting the CII at APSDC/ APSCAN.

8. Government after careful examination, hereby ordered that Non-Disclosure Agreement (NDA) shall not required to be signed by M/s APTS Ltd. to gather/ share information such as access credentials, documentation and all other IT infrastructure details for completion of Cyber Security Assurance Services.

9. All the Secretariat Departments/ HoDs/ PSUs/ Societies and Institutions etc., are therefore directed to approach M/s APTS Ltd. to avail the Cyber Security Assurance Services.

10. This Government Order shall come into force with immediate effect.

(BY ORDER AND IN THE NAME OF THE GOVERNOR OF ANDHRA PRADESH)

KVIJAYANAND
PRINCIPAL SECRETARY TO GOVERNMENT

To:

All the Spl. Chief Secretaries/ Prl. Secretaries/ Secretaries/ Spl. Secretaries to Government

All the Heads of Departments

All the District Collectors & Magistrates, AP

All the Societies/Institutions/Autonomous Bodies

The CEO, e-Pragati

The MD, AP State Fibrenet Ltd

The CEO, AP Core Digital Data Authority

The CEO, RTGS

The Managing Director, APTS Ltd.

All the Vice Chancellors of Universities in Andhra Pradesh

The Commissioner, I&PR, Vijayawada

Copy to:

The PS to Hon'ble Chief Minister, Andhra Pradesh

The OSD to Hon'ble Minister for ITE&C Department, Andhra Pradesh

The PS to Chief Secretary to Government of Andhra Pradesh

//Forwarded :: by Order//

SECTION OFFICER