

**GOVERNMENT OF ANDHRA PRADESH**  
**ABSTRACT**

ITE&C Department – Andhra Pradesh Cyber Security Policy 2017 - Orders – Issued.

---

**INFORMATION TECHNOLOGY, ELECTRONICS & COMMUNICATIONS (INFRA) DEPARTMENT**

G.O.MS.No. 2

Dated: 01-03-2017

Read the following

1. G.O. Ms. No.7, dated 19.05.2006 of IT&C (Infrastructure) department.
2. “National Cyber Security Policy in 2013”, notified in the Gazette of India Extraordinary No. 143, dated 02.07.2013.

**ORDER:**

**1. Context and Vision of AP Cyber Security Policy 2017**

Information and Communication Technologies have brought about transformative changes in all the sectors of the society and the economy. The exponential growth of the Internet technologies, and specially the SMAC technologies, has made the digital way of life the ‘new norm’, aided by the tremendous spread, reduced cost and ease of use of connected devices. Internet has given voice to the voiceless, power to the underprivileged and agility, efficiency and transparency to the Governments and businesses. The cutting edge technologies based on IoT and IoE are going to further revolutionize our way of life by connecting everything digital.

The spread of Internet and its indispensability bring with them a wide range of risks to the information on which rely the risk of loss, damage and misuse of valuable information- which can be of disastrous consequences to individuals, businesses and Governments. While it is not necessary to recount the nature and variety of such risks and threats, suffice it to say that an immense responsibility lies on individuals, businesses, the civil society and the Government to bring about a ‘cultural change’ in their approach to cyber security, to create systems for the prediction, prevention and remediation of any breaches to cyber security and to build a strong eco-system for detection, investigation and prosecution of cybercrime.

With the aforesaid objective in view, 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’*. These strategies seek to create an assurance framework; strengthen the regulatory framework; create capabilities and systems required for assessment of risks, early warning and incident management; protect Critical Information Infrastructure; secure e-Government services; develop human resources, and above all, create an all-round awareness of the importance of cyber security.

**P.T.O**

The State of Andhra Pradesh has been a pioneer in the use of ICTs extensively for delivery of public services. The **e-Pragati** Program being currently implemented by the Government is based on a whole-of-government approach, whereby all the e-Governance systems are interconnected and integrated and provides a wide range of services online. Core datasets like the People Hub, Land Hub, Entity Hub, GIS Hub and IoT Hub will be created and extensively used in providing digital services. The **AP FibreNet** initiative will make universal access to Internet a reality soon. In this context, it is all the more necessary for Andhra Pradesh to fortify its cyber security mechanisms and create a robust security ecosystem in the State.

The Government feels it expedient to establish the Andhra Pradesh Cyber Security Policy, to complement and supplement the National Cyber Security Policy 2013, and to give a practical effect to it in the State.

The Vision of the Andhra Pradesh Cyber Security Policy is 'to create a robust cyber ecosystem, wherein the **citizens** transact online securely and take steps to protect their identity, privacy and finances online, the **businesses** conduct their operations without any disruption or damage and the **Government** ensures that its data and ICT systems are secure'.

The Policy outlines the specific steps and initiatives to be taken by the Government and all other stakeholders to realize the Vision stated above.

## **2. Establishing Cyber Security Framework:**

- a. The Government shall create a **Cyber Security Framework** (CSF) in collaboration with the private sector. The framework shall have the following objectives and features:
  - i. The Framework shall be designed to address and manage cyber security risk in a cost-effective manner and shall guide all cyber security activities, while balancing the need to protect individual privacy;
  - ii. The Framework shall consist of a set of standards, guidelines and practices, which can be adopted by all organizations, irrespective of size, degree of cyber security risk or sophistication of its operations;
  - iii. The Framework shall be a living document that will evolve with time and get enhanced with emergence of new technologies and, alongside, new threats;
  - iv. The Framework shall cater to the entire **life cycle of cyber security** management, namely,
    1. **Identification of risks**, including inventorizing the assets – physical and digital, identifying critical business functions, assessing risks relating to the assets and business functions, and putting in place an appropriate risk management strategy and a governance mechanism for the same.
    2. **Protection of Assets**, including creating systems for access control and data security, establishing Standard Operating Procedures and deploying protective technologies.
    3. **Detection of Cyber security Incidents**, including monitoring and analysis of anomalies and events.

::3::

4. **Response to the Incidents** including response planning, communications strategy, mitigation and improvements for future resilience.
  5. **Recovery from the impact of the incidents**, including recovery planning, enhancements to systems and updates through immediate communications.
- b. As a sequel to the publication of the CSF, the Government shall also prepare a Blueprint and a Roadmap for implementing the CSF. The effort shall also include defining metrics for measurement of progress and the development of **Cyber Security Index** to be monitored at defined frequency.
  - c. The CSF may include provisions for reporting and disclosure norms, to be adopted on a voluntary basis, by all organizations dealing with in or IT. In particular, all the companies doing business with the Government shall be required to comply with the CSF mandatorily. Suitable provisions shall be incorporated in all RFPs relating to all major public procurements.
  - d. The Government shall endeavour, working with the industry, to publish the CSF the Blueprint and the Roadmap within 6 months of notifying this policy.

### **3. Securing the 'Government Cyber Space'**

The Government shall ensure that its data and ICT systems are secure in all respects and infuse trust and confidence in all the users, internal and external, to interact with the Government online. To this end, the Government will undertake the following activities:

- a. **Secure online services:** All the Government functionaries and their service providers shall ensure that the data and the ICT systems under their control that provide or support provision of online services mandatorily adopt the appropriate information security policies and practices at all times, in conformity with the CSF. This shall apply to all users, all personal devices and complex systems already installed or to be deployed in future. Security Audit in conformity with the relevant and applicable international standards shall be mandatory for all websites, applications and apps before they are hosted and published for internal or external use. To this effect, clear lines of responsibility shall be established as part of the Security plans of all organizations.
- b. **e-Pragati Security Architecture:** The Government has approved the massive program of e-Pragati, designed adopting the framework of Enterprise Architecture, which seeks to develop and deploy enterprise systems to provide all services online in an integrated manner. Implementation of e-Pragati entails a significant responsibility on all the Departments and their system integrators and service providers to conform to the international standards of information security. As a part of the e-Pragati Program, the Government shall design, develop and deploy a holistic and prioritised **e-Pragati Security Architecture**. The Government shall also establish an institutional mechanism for **e-Pragati Security Governance**, under an **e-Pragati Chief Information Security Officer**.

**P.T.O**

- c. **AP-CERT:** The Government shall establish the **AP Computer Emergency Response Team (AP-CERT)** in tune with the national and international norms, as the State-level coordination point for providing cyber security information and advice to the Andhra Pradesh community.

The AP- CERT shall operate in conjunction with Indian Computer Emergency Response Team (I-CERT) to respond to cyber security threats rapidly and effectively by coordinating security efforts and incident response for cyber security problems at the State level and to enhance the security of the State Communications and Information Infrastructure through proactive action and effective collaboration. The AP-CERT shall also oversee the implementation of crisis management plan.

AP-CERT shall have the following mandate:

- i. Collaborate with I-CERT and other CERTs in India to operate cohesively towards the mission.
- ii. Serve as central point in the state for responding to cyber security incidents when they occur and report all cyber security incidents to I-CERT
- iii. Initiate proactive measures to increase awareness and understanding of cyber security issues
- iv. Serve as a central point in the state for identifying and correcting vulnerabilities in ICT systems
- v. Provide a reliable, trusted, 24-hour, single point of contact for emergencies, by establishing a Security Operations Centre (SOC).
- vi. Help create trust in the electronic environment within the state
- vii. Implement Crisis Management Plan for the state
- viii. Provide, through a dedicated website, the AP Community with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect themselves;

The AP-CERT shall be an autonomous body to be established by the IT, Electronics and Communications Department and shall be headed by a Director.

- d. **Coordination with ISPs:** The Government shall coordinate with all the ISPs operating in the State to ensure that they establish and enforce appropriate cyber security plans in line with this policy.

- e. **Strategy on Security of Identities:** The Government shall put in place an appropriate strategy and implementation mechanisms to prevent digital impersonation and identity theft and the security incidents resulting therefrom. The strategy shall address inter alia, the following aspects:

- i. establishing strong authentication mechanisms, following the National e-Pramaan Policy and Standard;
- ii. prescribing enhanced security features on the statutory documents issued by the Government, to prevent forgery;

- iii. ensuring accuracy, secure access and privacy of the identity information held by the Government;
  - iv. promoting and/or mandating as the case may be, of the use of Digital Signature Certificates, operating under the Public Key Infrastructure framework, for the approval of specified categories of electronic transactions, documents and files and
  - v. use of bio-metric authentication systems in all transactions with government
- f. **Security Assurance Framework:** A framework of assurance shall be established, involving
- (i) the preparation of a panel of agencies, possessing the specified security certifications and other qualification criteria and
  - (ii) prescribing the requirement for the mandatory security audit of all ICT systems, Projects and applications deployed by the Government agencies, at such frequency as may be specified.
- g. **Budget:** All Government agencies implementing IT Projects shall earmark **5% of the annual IT Budget** towards compliance with the security requirements of IT Act 2000 and this Policy, and utilize the same for meeting the cost associated with, *inter alia*, preparation and implementation of cyber security plans and Information Security Management System (ISMS); procuring products required to provide cyber security for the information and assets; conducting of training programs on cyber security and for conducting security audit of systems required under this policy.

#### 4. Protection of Critical Information Infrastructure (CII):

- a. The AP-CERT shall work in close coordination with the **National Critical Information Infrastructure** Protection Centre, which has the responsibility of monitoring the Critical Information Infrastructure on a 24x7 basis from the perspective of cyber security and to alert the CISOs of the concerned establishments of any impending cyber threats and to advise and support them in undertaking preventive and remedial measures.
- b. Cyber security drills shall be carried out in all the identified establishments at the defined frequency, under the supervision of the I-CERT. The drills shall be cross-sectoral for experience sharing.
- c. AP Information Sharing Network for CII (AP-ISN) shall be established as a Community of Interest. The AP-ISN shall work in close coordination with the AP-CERT and
  - i. provide guidance and advice to APISN member organisations on control systems security in the form of advisories and alerts on specific vulnerabilities and threats to control systems and networks;

- ii. establish a SCADA Community of Interest to act as a forum to raise the awareness of security for control systems practitioners from critical infrastructure sectors, vendors, consultants and researchers, and
- iii. support control systems practitioners participating in training programs in advanced control systems cyber security.

**5. Enhancing Awareness of Citizens and Small Business:** The Government shall take the following steps for enhancing the awareness of citizens and small business in all areas concerning cyber security to be practiced at their level.

- a. Build a **single reporting system** for citizens and small businesses to report cyber incidents so that action can be taken by the law enforcement agencies. **A Cyber Security Call Centre** will be established with a toll free number, which the citizens can call to get help and support on security incidents.
- b. Launch a web-site [www.onlinesafe.org](http://www.onlinesafe.org), on a PPP basis, for providing up-to-date advisories to the citizens and small business on safe practices while transacting online and to provide the registered members alerts on guarding against the anticipated threats.
- c. Undertake an awareness campaign on cyber security through workshops, advertisements in print and electronic media and through short videos published on all frequently-visited web-sites.
- d. Establish a cadre of **Web Constables** from the citizenry, who have the specified qualifications and who volunteer to provide advocacy and reporting services to the community on specified aspects of cyber security and crime, in close association with the local police.
- e. Promote a **Cultural Change** such that every citizen believes that **cyber security begins at home** and that they have the necessary basic knowledge to apply simple security procedures on all the digital devices that they operate.

**6. Capacity Building:** Capacities for managing the cyber security have to be built at various levels, considering the increasing sophistication of cyber threats and crime and the burgeoning size of user base of digital equipment and devices. The following steps shall be taken to address the capacity needs at various levels and in various areas of cyber security.

- a. **20,000 Cyber Security professionals** will be trained over the next 5 years – 500 at Masters level, 10000 at the Graduate level, 4500 from among the employees of the State Government and 5000 employees working in the private sector. This program shall be formulated and implemented in close association with the ongoing Phase II of the ISEA (Information Security Education and Awareness) Program of the Ministry of Electronics and IT, Government of India.
- b. Changes will be made in the curriculum of the schools, colleges and Universities so as to enhance awareness of cyber security among school students, general cyber security skills among college students and advanced knowledge of cyber security among the university students.

- c. The following certification courses will be introduced in the Universities, which can be availed by graduates in Computer Sciences:
  - i. Masters Program in Cyber Security
  - ii. Masters Program in Cyber Forensics
- d. **Annual Conference on Cyber Security:** Starting 2017, the Government shall promote holding of an Annual Conference on Cyber Security in a PPP mode, to reinforce its commitment to cyber security and provide an impetus to the multiple initiatives in this area.
- e. **Collaboration:** Given the evolving nature of cyber security, and the need for enhancing the efforts in R&D and innovation in this area, the Government intends to establish a strong eco-system for Academia-Industry-Government collaboration. The outcomes envisaged include the establishment of Cyber Security Labs in all the universities, a few Centres of Excellence in different areas of cyber security and building a Cyber Range.
- f. **Secure Software development:** A Centre of Excellence in Secure Software Development shall be established as a part of the International Institute of Digital Technologies, Tirupati, with the motto "**Secure by Design**".

**7. Strengthening the Law Enforcement Agencies:** The following initiatives shall be taken by the Law Enforcement Agencies in the State over a 3-year period:

- a. All the Police Officers of the rank of **Sub-Inspector and above**, shall be imparted training in Cyber security, through courses ranging from 2-weeks to 3-weeks, depending upon the needs of different categories of police functionaries, with focus on the areas of prevention, investigation and prosecution of cybercrimes.
- b. Since combating cybercrime is an ever-changing challenge, the training programs will be planned on a continuing basis.
- c. An appropriate institutional mechanism will be established for undertaking these training programs in a structured manner.
- d. The Law Enforcement agencies will be permitted to retain the services of Cyber Security Professionals in the private sector, to assist and advise them in tackling organized crime and handling complex cases involving cyber forensics.
- e. Police Officers well-trained in cyber security shall be posted in the security establishments of the sectors categorized as Critical Information Infrastructure.
- f. Cyber Police Stations and Cyber Forensics Labs will be established in all the major Cities of the State.
- g. Police Officers specializing in cyber security will be encouraged to participate in global conferences on cyber security.

**8. Partnerships:** The Government recognizes that the complexity and size of the task in guarding against cyber threats is too large for it to manage by itself. To this end,

**P.T.O**

::8::

Government shall partner with the private sector and the academia through a set of specific programs, which inter alia, include the following:

- a. Capacity Building to create a 20000-strong cadre of Cyber Security professionals in the State in 5 years;
  - b. Promoting the establishment of the position of Chief Information Security Officer in all organizations, with the overall responsibility for managing cyber security in respect of all the cyber-assets of the organization and for protecting the privacy of Personal Identification Information held by the organization;
  - c. Conducting training programs and workshops for the IT Professionals of the public and private sectors, to impart them skills in secure programming and development of secure applications and apps;
  - d. Promoting the creation and active functioning of Information Sharing and Analysis Centres (ISACs) in the private organizations that supplement the efforts of the Government in addressing issues concerning cyber security.
- 9. Promoting Cyber Security Industry in AP:** The Government shall notify an appropriate policy of incentives and other facilitatory mechanisms for developing AP as the preferred destination for the cyber security industry, and eventually, to establish a globally reputed **Cyber Security Hub** in AP.
- 10. Review of the Policy:** In so far as cyber security is an evolving field, the requirements keep changing on a continuous basis. Keeping this in view, the AP Cyber Security Policy shall be reviewed and enhanced on a bi-annual basis.

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

K.VIJAYANAND  
**PRINCIPAL SECRETARY TO GOVERNMENT (FAC)**

To  
All the Departments of Secretariat  
All the District Collectors & Magistrates, AP  
All the HoDs  
The CEO, eGovernance Authority, GoAP  
The Managing Director, M/s APTS Ltd.

Copy to:  
The PS to Hon'ble C.M., Andhra Pradesh  
The OSD to Hon'ble Minister for Information Technology, Andhra Pradesh  
The PS to Hon'ble Minister for Finance, Andhra Pradesh  
The PS to PFS, Andhra Pradesh  
The OSD to JS to Hon'ble CM, Andhra Pradesh  
The PS to Chief Secretary to Government of Andhra Pradesh

//FORWARDED::BY ORDER//

**SECTION OFFICER**