

GOVERNMENT OF ANDHRA PRADESH
ABSTRACT

Information Technology Security Policy of the Government of Andhra Pradesh –2006 - Orders – Issued.

INFORMATION TECHNOLOGY & COMMUNICATIONS DEPARTMENT
Infrastructure Section

G.O Ms. No. 7

Dated : 19.05.2006

ORDER :

Andhra Pradesh Secretariat forms the data & security hub for A.P. Government transactions. IT Security Policy plays a major role in ensuring that the sharing and accessing of information over the Government networks is secure and also to ensure optimum utilization of hardware and software resources. Considering the various services and the steps taken by the Government of Andhra Pradesh towards e-Governance and the reach of IT to every citizen, it is highly necessary to focus on data security for secured access. The IT Security Policy has been defined with the thought to bring in awareness among the employees and the concerned department about the importance of data and the method to keep it safe at various levels. IT Security Policy also aims at educating employees and other users on the methods of safeguarding the data and confidential information from being exposed to outsiders through any means.

2. Policies are used as a reference point for a wide variety of information security activities including designing controls into application systems, establishing user access controls, performing risk analysis, conducting computer crime investigations etc. Presently there is no Security Policy and no Security Organization within the Government. As per BS7799 Security Standards, every organization/enterprise should have Security Policy and a high level IT Security Steering Committee to oversee the issues related to IT Security. Policies are the primary building blocks for every successful information security effort. In order to be successful, every information security effort needs to have a set of policies, which provides clear instructions and establishes management support.

3. An Information Security Policy document is essential for many reasons. Beyond the definition of roles and responsibilities for employees, a policy document sensitizes employees to the potential problems associated with modern information systems. This education and training helps minimize the cost of security incidents, helps accelerate the development of new applications systems, and helps assure the consistent implementation of controls across an organizations' information systems. Information security policies are also important reference documents for internal audits and for the resolution of legal disputes about managements' due diligence. Policy statements can also serve as evidence of managements' intention to safeguard organizational information; this is an essential but often neglected step in the legal assertion of trade secret protection. An information security policy document can further more serve as evidence of internal quality control processes.

4. A brief description and benefits of IT Security Policy is placed at APPENDIX-I and the IT Security Policy is placed at APPENDIX-II.

5. This policy will be enforced with effect from date 19.05.2006. The Steering Committee under the chairmanship of Pri. Secretary IT&C Department will be responsible for reviewing the implementation mechanism and take up timely corrective measures. The Steering Committee shall meet atleast once in 3 months. The Apex Committee under the chairmanship of Chief Secretary will be responsible for any major changes that need to be incorporated in the Security Policy based on the experience gained in its implementation. It will advise HODs from time to time on ensuring effective security environment of the LANs/WANs in their Departments / Corporations so that the policy guidelines are enforced in all Government Departments / Agencies.

:: 2 ::

6. This order does not require the concurrence of the Finance Department.
7. This order is available online at URL <http://www.apit.gov.in>

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

T.K.DEWAN
CHIEF SECRETARY TO GOVERNMENT

To

All Departments of the Secretariat
All HODs

// FORWARDED: BY ORDER//


SECTION OFFICER


Brief Description & Benefits of IT Security Policy

1. Brief Description of IT Security Policy

The Security policy comprises of several areas of day-to-day working on computers, internal usage, physical security, networks and their management. Some of these are listed below with brief description.

Password policy – Minimum password length, limit on consecutive unsuccessful attempts.

System Usage policy – Screen savers, logging off PCs, sharing of folders, storing of games, shifting of PCs.

E-Mail Policy – Legal disclaimer notice, chain mails, broadcast mails, obscene, profane or derogatory remarks, size limit on attachment and mailboxes.

Anti Virus Policy – Virus checking, system sharing, suspected mails, virus eradication.

Internet policy – Internet use for personal purpose, appropriate behavior, blocking of objectionable and unsafe sites, misrepresentating user identity.

User Policy – Transfer of GoAP information, gaining unauthorized access, notification of suspected loss or disclosure of sensitive information.

Data Security policy – Identification of vital records, downloading of sensitive information, backup of critical data, disposal of removable media.

Physical Security Policy – Physical security of sensitive information, intrusion alarms, physical access control, locking of rooms.

Prohibition and Approval Policy – Communication changes, setting up of multi user systems, in-house system interconnection.

Process related policy – Reporting of security incidents, confidentiality, agreements, information security trainings, ownership of systems.

Telecommuting Policy – Safety, exclusive usage, configuration changes.

Administrator Policy – Approvals, privilege restriction, dormant users, security violations, data backup, security alert, periodical testing of backup procedures.

Network and Firewall Security Policy–DMZs, auditing, intrusion detection, vulnerability monitoring.

Asset Classification & Management – Third party access, asset classification, incident handling, secure disposal, cryptography controls.

Management of Security policy – Apex and Steering Committee, security organization.

2. **Benefits of IT Security Policy:**

(a). System Policy :

- It would be easier for system identification, tracking the system, asset management and trouble shooting.
- By using boot password, it provides unauthorized logins.
- Useful for maintaining hardware and software asset list in a centralized manner.
- By having unique login username and password, the privacy and security of the information in the system is enhanced.
- With the antivirus software gives increased information security protection, stability of the system and prevents data loss.

(b). Network and Firewall Security Policy :

- Monitoring and maintenance of the network would be easier.
- Isolation of the network would be easier during the time of heavy broadcast and any major virus attack.
- Performance and management of network will be improved by using the VLANs.
- Monitoring of inbound and outbound traffic would detect suspicious network activities and illegal network penetration, which can be blocked.
- By using content inspection, it can block all vulnerabilities in the entry point itself.
- By integrating firewall with NIDs, all suspicious activities and intrusions would be blocked and monitoring would be easier.
- Bandwidth utilization reports would be generated and controlled.
- Network would be more secure when ISP entry points are integrated with firewall ,antivirus wall and NIDs.
- By using VPN connectivity network access from outside users would be secured.
- The network activities of users can be monitored easily in VPN and dial-up connectivity.
- Daily virus block logs can be monitored by integrating gateway with antivirus wall.

(c). User Policy :

- Identification of users would be easier, if the username is relevant to their department designation.
- Data security and virus protection is increased by not sharing the files or folders.

**T.K.DEWAN
CHIEF SECRETARY TO GOVERNMENT**

// FORWARDED: BY ORDER//


SECTION OFFICER