

1.0 Purpose

All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Personnel security is necessary to uphold access control and to limit information retrieval to a need-to-know basis.

2.0 Scope

This standard statement applies to all state agencies, institutions of higher education, boards and commissions.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies.

4.0 References

- 4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.
- 4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

- 5.1 Each affected organization shall implement an ongoing IT security awareness program which communicates the IT security policy to each user and promotes a complete understanding of the importance of IT security. It should convey the message that IT security is to the benefit of the organization and all its employees, and that all employees are responsible for IT security.

- 5.2 IT management should ensure that their personnel, including contracted personnel, are subjected to an appropriate level of security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. An employee who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

- 5.3 IT management should maintain a record of individuals currently authorized to access sensitive information.

6.0 Procedures

The agency shall be able to demonstrate compliance with this policy.

7.0 Revisions

None

8.0 Definitions

- 8.1 Training: Any information sharing, orientation process, ongoing supervision, or counseling. This may also include training by methods of an informal classroom, the intranet, and any posted internet information.
- 8.2 Security Clearance: Security clearance may include a law enforcement background check and may be combined with some form of biometric identification (i.e., fingerprints)

9.0 Related Resources

- COBIT Standards:
<http://www.isaca.org/cobit.htm>
- HIPAA Final Security Standards:
<http://www.hipaadvisory.com/regs/finalsecurity>
- United States Department of Agriculture's Personnel Security Process:
<http://www.usda.gov/da/pdsd/>

State of Arkansas Office of Information Technology



State Security Office

www.cio.arkansas.gov/security

PERSONNEL SECURITY

People are an important part of an effective security strategy. Technology alone cannot protect sensitive or critical information. Statistics show that a majority of system compromises come from within organizations, but it is not always an intentional act. The more aware a person is about secure information technology behavior, the stronger the organization's cyber defenses will be.



Proper security screening of personnel (including contract personnel) is a necessity prior to allowing access to computers and network systems. Varying levels of security clearance may be based on the sensitivity of the employee's position.

Security clearance checks include law enforcement background checks and biometric identification (fingerprints, etc.), and IT management must maintain records of individuals currently authorized to access sensitive information.

END USER AWARENESS

Education of personnel regarding IT security is an essential and effective way to prevent damage and destruction to computer systems. There are many ways to accomplish this, such as new employee orientations, ongoing supervision, informal classroom presentations, an office intranet, and any internet information.

Without employee awareness and cooperation, organizational networks are at high risk. End users may become victims of scams, may be fooled by social engineering that entices them to dangerous web sites or to open malicious email, or may have illicit spyware or adware remotely loaded from an Internet site.

In surfing the Internet, small self-contained programs are often downloaded to a computer, usually without permission. These automatically take action on a computer, such as deleting files, modifying the computer's settings, stealing passwords and sending ad hoc emails.

Few people realize that by simply visiting a website or opening an email, much of this undesirable activity can automatically occur on their computer and that anti-virus software protection is not enough.

AVOID PROBLEMS

In a work environment, the risks multiply. Employees enter passwords to access a variety of systems, applications, and accounts that contain sensitive data. They also share private information with co-workers and partners via email . . . even as spyware records every keystroke and passes it along to a faceless third party.

Some ways to avoid problems:

- Only install software from trusted sites and vendors.
- Think before responding to requests for information. Email sender names can be spoofed and bad websites can look like legitimate ones.
- Avoid peer-to-peer (P2P) activity which gives other people's computers access

to the files on your computer, unless your organization trusts the others in the P2P network.

- Read end user license agreements before accepting them. Look for wording that describes information gathering capabilities and be wary of agreements that are extremely lengthy or ambiguous.
- Use spyware prevention and eradication software; virus detection alone will not work.
- Regularly delete unwanted cookies. A cookie is information that a website puts on your computer so that it can remember something about you or your computer later. Utilities are available that can delete cookies with just one or two mouse clicks.
- Use a personal firewall that monitors when any application attempts to access the Internet.



QUESTIONS?

If you have questions about Personnel Security standard, please contact:

- Arkansas State Security Office
(501) 682-4300
sso@mail.state.ar.us
www.cio.arkansas.gov/security

If you have questions about personnel security issues, please contact:

- Your Network Administrator or IT Support Staff