

1.0 Purpose

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Virus scanning software has proven effective in protecting state resources from viruses, worms, and other types of malicious code.

2.0 Scope

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

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 oversee the development of information technology security policy for state agencies.

4.0 References

- 4.1 Arkansas State Government Information Resources Security Policy Guidelines
- 4.2 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.
- 4.3 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

- 5.2 All microcomputer workstations and servers attached to the state network shall have updated virus protection software installed and enabled.
- 5.2 At a minimum, virus definitions shall be updated weekly.

6.0 Procedures

The agency shall be able to demonstrate compliance.

7.0 Revisions

None

8.0 Definitions

- 8.1 **Virus:** A programming code usually disguised as something else that causes some unexpected and usually undesirable event. It is often designed so that it automatically spreads to other computer users. Viruses can be transmitted as attachments to an e-mail, as downloads, or be present on a diskette or CD. The source of the e-mail, downloaded file, or diskette is often unaware of the virus.
- 8.2 **Worm:** A self-replicating virus that does not alter files but resides in active memory and duplicates itself; operates through automatic parts of an operating system and is usually invisible to user.
- 8.3 **Workstations and Servers:** In this standard, workstations and servers are defined as computers that are capable of becoming infected with a virus, worm, or other malicious code.

9.0 Related Resources

Antivirus software links:

Norton Antivirus: <http://www.symantec.com/nav/>

McAfee Antivirus:
<http://www.mcafee.com/anti-virus/default.asp>

Hoaxes:
<http://hoaxbusters.ciac.org/HoaxBustersHome.html>

AVG Antivirus:
http://www.grisoft.com/html/us_index.htm

eTrust:
<http://www3.ca.com/Solutions/ProductFamily.asp?ID=128>

VIRUS SCANNING

State of Arkansas

Office of the Executive
Chief Information Officer

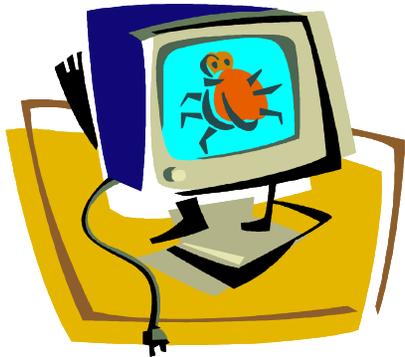


State Security Office

VIRUS SCANNING

Virus scanning is an effective way to prevent damage and destruction to your computer system caused by worms, viruses, and other types of malicious code.

There are numerous effective virus scanning products available to users and organizations that have been proved successful in preventing unwanted attacks.



VIRUS SCANNING REQUIREMENTS

State security standard requires agencies to adhere to these two (2) rules:

- All workstations and servers must have updated virus protection software installed and enabled.
- All virus scanning software must be updated weekly.

HOW DO VIRUSES SPREAD?

- **Email** is a favorite method of spreading virus infections. The most common form of email attack is through attachments.
- **Embedded code** is another method of spreading virus infections through email. These attacks are “invisible”. Malicious code is actually built into the email rather than using an attachment.
- **Diskettes & CDs** can also harbor and transmit viruses.

Often, the source of the email, diskette, or CD is unaware of the virus.

TIPS FOR EFFECTIVE VIRUS SCANNING & CONTROL

- Keep current on virus alerts issued by reputable virus software vendors. Be aware of the latest virus attacks and hoaxes.
- Avoid opening attachments from unknown sources or those with suspicious extensions (i.e., .bat, .eml, .exe).
- Consider disabling the preview window. Some malicious codes will activate if previewed.
- Notify your system administrator immediately if you think you have received a bogus attachment or have a virus on your system.



QUESTIONS?

If you have questions about Virus Scanning standards contact:

- Arkansas State Security Office
(501) 682-4300
StateSecurityOffice@arkansas.gov
www.cio.arkansas.gov/security

If you have questions about virus scanning problems please contact:

- Your Network Administrator / Information Technology Support Staff
- The Department of Information Systems' Customer Care Center
(501) 682-HELP (682-4357)
DIS.CallCenter@mail.state.ar.us
www.dis.state.ar.us/care_ctr