State of Arkansas
Office of the State Executive Chief Information Officer
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Agency #200-00

Best Practices Statement – Instant Messaging Security

Title: Instant Messaging Security

Document Number: BP-70-020

Effective Date: 9/15/2005

Published by: Office of Information Technology

1.0 Purpose

Instant messaging is an alternate way for people to communicate with each other using their personal computers, but instant messaging can be a conduit for malicious software to infect users' machines. While instant messaging has benefits, it should be utilized in a controlled manner to protect state resources.

2.0 Scope

This best practices statement is recommended for all state agencies, 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 oversees the development of information technology security policy for state agencies. The State Security Office, under the state's Executive Chief Information Officer, defines an environment for strategic security architecture and sets security standards and policies for information technology in state government. In order to apply appropriate security measures, data must first be classified to determine its sensitivity and required availability.

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.

4.3 Virus Scanning Standard: http://www.cio.arkansas.gov/techarch/indexes/standards.htm

5.0 Best Practices Recommendation

5.1 Organizations should use private instant messaging programs, which are closed systems, instead of public instant messaging programs.

5.2 Current antivirus software should be used on all machines using instant messaging software.

5.3 File sharing with computers external to agencies should be blocked on machines utilizing instant messaging software.

5.4 Computers should be configured to only receive messages from known entities.

5.5 Agencies should only use instant messaging programs that allow users to block file sharing.

6.0 Revision History

Date	Description of Change
9/15/2005	Original Best Practices Statement Published

7.0 Definitions

7.1 Instant Messaging

Instant messaging is the ability to instantly communicate with another person with text messages on personal computers. Utilizing the same instant messaging software, both users must be online at the same time to communicate. Software does exist that bridges different types of instant messaging software. Some instant messaging software allows the exchange of files and voice messaging.

8.0 Related Resources

9.0 Inquiries

Direct inquiries about this best practice recommendation to:

Office of Information Technology
Shared Technical Architecture
124 West Capitol Avenue Suite 990, Little Rock, Arkansas 72201
Phone: 501-682-4300
FAX: 501-682-2040
Email: SharedArchitecture@arkansas.gov

OIT policies can be found on the Internet at: http://www.cio.arkansas.gov/techarch