State of Arkansas **Agency 200-10**
Office of Information Technology
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Standard Statement – Spyware Scanning

Title: Spyware Scanning

Document Number: SS-70-005

Effective Date: 9/1/2006

Published by: Office of Information Technology

1.0 Purpose

Spyware poses a significant threat to publicly-owned computers attached to the Internet due to its malicious nature. Spyware is capable of stealing information from computers, changing computer settings, logging keystrokes, and other nefarious actions without the user's knowledge. Oftentimes, antivirus software does not block spyware from infecting computers and, for this reason, technology must be used to detect, prevent, and clean spyware from machines. Arkansas government collects personal information and this information must be protected from disclosure.

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 All publicly owned microcomputer workstations and servers attached to the state network that are susceptible to infection by spyware shall have updated anti-spyware software installed and enabled.

5.2 At a minimum, anti-spyware definitions shall be checked weekly for updated definition files and downloaded.

6.0 Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception to any part of this standard.

7.0 Revision History

Date	Description of Change
9/1/2006	Original Standard Statement Published

8.0 Definitions

8.1 Spyware:
Software that modifies, through intentionally deceptive means, settings on a computer such as which page appears when a user launches his browser, the default provider of Internet services, the authorized user's list of bookmarks used to access or search the Internet, or the file on a computer used to resolve a uniform resource locator. Spyware is also defined as software that collects personally identifiable information, through intentionally deceptive means, such as the key strokes of a user, all the Internet addresses visited by the user, screen shots for a purpose unrelated to the software, and other information from a user's hard drive. In general, spyware is any software that secretly gathers information in an intentionally deceptive manner from a user's computer.

9.0 Related Resources

9.1 www.stopbadware.org

9.2 www.spywarewarrior.com

9.3 Act 2255 of 2005 – An Act to Protect Consumers from the Improper Use of Computer Spyware : ftp://www.arkleg.state.ar.us/acts/2005/public/Act2255.pdf

9.4 "Recognizing and Avoiding Spyware," Cyber Security Tip ST04-016, National Cyber Alert System, US-CERT : http://www.us-cert.gov/cas/tips/ST04-016.html

10.0 Inquiries

Direct inquiries about this standard 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