

Standard Statement – Password Management

User Logon Passwords	Document Number: SS-70-002
	Effective Date: 12/14/2003
	Published By: Office of the ECIO

1.0 Purpose

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Effective controls for logical access to information resources minimize inadvertent employee error and negligence, and reduce opportunities for computer crime. Each user of a mission critical automated system is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access to automated information. Passwords are used to authenticate a user's identity and to establish accountability.

2.0 Scope

This standard statement applies to 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 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

- 5.1 At a minimum, passwords shall be changed every 90 days.
- 5.2 Passwords shall be at least eight characters in length and be a mixture of alpha and nonalpha characters
- 5.3 User passwords shall not be reused within six password changes.

6.0 Procedures

The agency shall be able to demonstrate compliance.

7.0 Revision History

Date	Description of Change
12/14/2003	Original Standard Statement Published

8.0 Definitions

- 8.1 Password:
A secret word or code used to serve as a security measure against unauthorized access to data.

9.0 Related Resources

Password selection guidelines:

<http://www.uic.edu/depts/accctest/accts/password.html>

http://www.ucolick.org/computing/password_selection.html

http://www.sans.org/resources/policies/Password_Policy.doc

10.0 Inquiries

Direct inquiries about this standard to:

Office of Information Technology
Shared Technical Architecture
124 W. Capitol Ave., Suite 200
Little Rock, AR 72201
Voice: 501-682-4300
FAX: 501-682-2040
Email: ITarch@mail.state.ar.us

OIT policies can be found on the Internet at:
<http://www.techarch.state.ar.us/>