State of Arkansas
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 – Physical and Logical Security

Title: Physical and Logical Security for Information Technology Resources

Document Number: SS-70-008

Effective Date: 05/01/2006

Published by: Office of Information Technology

1.0 Purpose

Information technology (IT) assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Physical 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 Data and System Security Classification Standard (SS-70-001): http://www.cio.arkansas.gov/techarch/indexes/standards.htm

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.

4.4 Arkansas General Records Retention Schedule.

5.0 Standard

5.1 Physical Security

5.1.0 The management of each covered entity is responsible for the implementation and maintenance of the physical security measures for their organizations.

5.1.0.1 Physical security and access controls shall address the areas containing system hardware, network wiring, backup media, and any other elements required for the system's operation.

5.1.0.2 Management shall establish appropriate physical safeguards over devices that provide physical or logical access to sensitive data and systems (Data and System Security Classification standard Levels B, C, and D).

5.1.1 Master copies of critical software (Data and System Security Classification standard Levels 2 or 3) shall be housed within a locked or otherwise restricted environment at all times allowing access to only those authorized by the covered entity.

5.1.2 All retired media must be processed so that no license-restricted software or sensitive data is retrievable.

5.1.3 Covered entities with systems classified by the Data and System Security Classification standard as Levels 2B, 2C, 2D, 3B, 3C and 3D shall:

5.1.3.1 Periodically update data backups.

5.1.3.2 House media containing backup data required for restoration within a locked or otherwise restricted environment in a building apart from the systems housing the data.

5.1.4 Access to backup media shall be restricted to only those authorized by the covered entity.

5.1.5 Covered entities shall secure network components including but not limited to servers, hubs, routers and switches within a locked or otherwise restricted environment at all times allowing access to only those authorized by the covered entity. New or substantially modified facilities shall incorporate lockable enclosures or closets for network layer components. Each state agency shall comply with the rules and guidelines promulgated under this subchapter upon the earlier of:

(1) July 1, 2007; or
(2) The line-item appropriation to the agency in question of funds to comply with this subchapter.

5.1.6 Server based applications with access to data classified as Levels C or D by the Data and System Security Classification standard shall:

5.1.6.1 Terminate client/server or server application sessions after a specific amount of inactivity as determined by the agency owning the application.

5.1.7 Reasonable measures must be taken to physically secure mobile computing and data storage devices such as laptops, personal digital assistants (PDAs) and flash drives from access by unauthorized users. Examples include, but may not be limited to:

5.1.7.1 Inventory control

5.1.7.2 Locked storage

5.1.7.3 Continuous possession in public places

5.1.8 Lock the screen of all devices that provide physical or logical access to sensitive data and systems (Data and System Security Classification standard Levels B, C, and D) after a maximum of 15 minutes of inactivity.

5.1.8.1 Continuously monitored workstations are exempt from this standard.

5.2 Logical Security

5.2.0 Access Control and Auditing

5.2.0.1 Management shall ensure each information asset (data and systems) has an appointed custodian, who could be a single person or group, who makes decisions about classification and access rights.

5.2.0.2 The logical access to and use of information technology computing resources shall be restricted by the implementation of authentication and authorization mechanisms linking users and resources with access rules based on the individual's demonstrated need to view, add, change or delete data.

5.2.0.3 Agencies shall maintain logs of logon attempts to all agency servers defined in the Data and System Security Classification standard for all classifications except 1A. Logs shall include user account name, the IP address, unsuccessful/successful attempts and time of occurrence. Covered entities shall determine the appropriate length of time to retain such logs. Agencies subject to the Arkansas Records Retention Schedule shall keep logs according to that schedule.

5.2.0.4 Data sent to an entity outside the scope of this standard shall have all sensitive data as defined in the Data and System Security Classification standard Levels C and D redacted or controlled under a nondisclosure agreement.

5.2.0.4.1 Data sent to an entity that already has the data is exempt from this standard.

5.2.1 User Account Management

5.2.1.1 Management shall establish procedures to ensure timely action relating to requesting, approving, establishing, issuing, suspending and closing of user accounts.

5.2.1.2 Management shall have a control process to identify inactive users and deactivate their access rights.

5.2.2 Violation and Security Activity Reports

5.2.2.1 Information technology security administrators shall ensure that significant violation and security activity is logged, reviewed, and appropriately reported and escalated to identify and resolve incidents involving unauthorized activity. Parties to which reports may be submitted could include agency management, agency IT personnel, the State Security Office, or law enforcement officials.

5.2.2.2 Known or suspected penetration of the covered entity's system security that attempts to compromise systems within local area networks shall be reported to the State Security Office, unless precluded by law enforcement, within one business day of the discovery of the incident.

5.2.3 Firewalls

5.2.3.1 Covered entities shall use firewall(s) that are appropriately configured to protect information technology resources.

6.0 Procedures

6.1 Agencies shall be able to demonstrate compliance. Covered entities are also subject to audit by the Arkansas Division of Legislative Audit for compliance with COBIT guidelines. Agencies may also be subject to state and federal law, rules and regulations that are more restrictive, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

6.2 Covered entities may report compromise attempts defined in 5.2.2.2 through a variety of means that may include calling, online reporting, or other methods of communication as defined by the State Security Office.

6.3 The State Security Office reserves the right to grant an exemption to any part of this standard.

7.0 Revision History

Date	Description of Change
05/01/2006	Promulgated

8.0 Definitions

8.1 Firewall:
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware or software, or a combination of both.

8.2 Client/Server:

A Client/Server architecture provides a scalable architecture, whereby each computer or process on the network is either a client or a server. Server software generally, but not always, runs on powerful computers dedicated for exclusive use to running business applications or storing data bases. Client software on the other hand generally runs on common PCs or workstations. Clients get all or most of their information and rely on the application server for things such as configuration files, business application programs, or to offload computer-intensive application tasks back to the server in order to keep the client computer (and client computer user) free to perform other tasks.

8.3 Continuously monitored:

A workstation is attended at all times by at least one person.

9.0 Resources

9.1 COBIT Standards: http://www.isaca.org/cobit.htm

9.2 HIPAA Security Standards: http://www.hipaadvisory.com/regs/finalsecurity/

9.3 CERT Physical Security Guidelines:
http://www.cert.org/security-improvement/practices/p074.html

9.4 OIT data erasure guidelines: http://www.cio.arkansas.gov/oit/AgPlan/Policies/comp_recyc.htm

9.5 M & R guidelines: http://www.arkansas.gov/dfa/procurement/mr/pro_mr.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