Physical and Logical Security Standard Guidelines

Document Number SS-70-008

State of Arkansas - Office of Information Technology

Physical and Logical Security Recommendations

Physical security is an essential part of information technology security. Physical security encompasses not only the area containing system hardware, but also locations of wiring used to connect the systems, supporting services, backup provisions and any other part of the systems.

Laptops and other types of mobile computing devices must also be protected from theft. Oftentimes, the data on the mobile device is of more value than the device itself. The mobile devices themselves can also serve as an entry point onto the state network. Extreme care must be taken with devices containing sensitive state data and personal information. When information technology resources are located in a public place, they should be protected as well.

Logical security uses technology to allow individuals access to information and systems based on who they are and what their role is within an organization. Access to information technology resources should be restricted to only those individuals with a need for access. Determining information ownership, access rights and the process to monitor that individuals have appropriate access are all a part of an effective security strategy.

Requirements of the 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 should address the areas containing system hardware, network wiring, backup media, and any other elements required for the system's operation.

Agency management is ultimately responsible for an agency's security measures and should be aware of the existing locations of networking equipment and backup media to prevent unauthorized access or tampering. In order for agencies to recover from a disaster, appropriate personnel must know the location of their backup information and the software required to recover systems.

5.1.0.2 Management should 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).

Disclosed sensitive information can lead to identity theft and other serious consequences. Only approved personnel should have physical access to devices that provide physical or logical access to sensitive data and systems. Secured backup tapes, servers in locked rooms, workstations that lock while they are unattended, and locking cables for computers are all examples of physical ways to secure devices that provide physical and logical security.

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

Securing master copies of critical software ensures that the software won't be used illegally or be used to gain unauthorized access to agency applications. The master copies are also needed to recover software in the event a computer requires its software to be reloaded.

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

Sensitive information must not be recoverable from retired media. **Instructions for the disposition of hard drives** have been published by the Office of Information Technology. In addition, the Office of Information Technology has released other **cleaning guidelines** for differing types of data storage devices.

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.

Agencies should refer to the Data and System Security Classification standard to classify their organizational information. Data classified as 2B, 2C, 2D, 3B, 3C, or 3D are subject to section 5.1.3.1 of the Physical and Logical Standard. Since accurate, current data is necessary to recover from some security incidents and other disasters, backups should always be current to avoid lost work. Agencies ultimately determine the frequency of backups taken of their organization's data.

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.

To ensure safety and availability of the backups, they must be stored offsite in a secure environment. Fires and other threats can destroy original data and backup data if they are held in the same location. Backup data should also be protected within a secure environment to protect the data from disclosure. Agencies may choose to also have a copy of backup data onsite to allow for faster recovery.

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

To prevent theft or misuse of information, only authorized personnel should have access to backups.

5.1.5 Covered entities shall secure all network layer 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 must 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.

Since hubs, routers and switches allow a computer to be physically connected to the agency network, they need to be secured in a restricted space with only authorized personnel having access. Servers should also be restricted to prevent tampering and possible compromise. Agencies have until July 1, 2007 to comply with section 5.1.5 or when they receive an appropriation to comply with section 5.1.5, whichever comes first.

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.

To prevent unauthorized access, applications must terminate if no activity occurs within a predetermined amount of time. Agencies determine the appropriate amount of time of inactivity allowed before terminating applications with access to data classified by the Data and System Security Standard as Levels C or D. Leaving applications with access to very sensitive or extremely sensitive data unattended provides opportunity for unauthorized users to “hijack” the session.

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 are not limited to:

5.1.7.1 Inventory control

5.1.7.2 Locked storage

5.1.7.3 Continuous possession in public places

Mobile computing devices are particularly vulnerable to theft because they are often used outside secured areas. Data on these devices is often worth more than the devices themselves. Extreme caution should be used when using mobile devices containing sensitive information. Laptops should not be visible in unattended cars.

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 manned workstations are exempt from this standard.

To prevent unauthorized access, the screen must lock with a password or other authentication method after a maximum of 15 minutes with no activity. When employees leave their workstations unattended, an unauthorized person can assume the same access rights as the employee. If someone is at the workstation at all times, which may be the case in a data center, it is not necessary to have the workstation restrict access to the application by complying with section 5.1.8.1.

5.2 Logical Security

5.2.0 Access Control and Auditing

5.2.0.1 Management should 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.

To prevent misuse of data, only personnel approved by the data custodian should be given access rights. Data custodians determine who has the right to read, write, change or delete information from agency files. Employees should be given the minimum necessary level of access to data and systems to perform their jobs.

5.2.0.2 The logical access to and use of information technology computing resources should 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.

Access to the state's network, state information technology resources, and state information should require authentication which is the process of proving who a person is through a mechanism, such as a password. Authorization gives employees the right to access resources such as printers, servers, and other peripherals as well as to read, write, change, or delete information. All users should be authenticated individually to allow for the auditing of their actions with computer resources.

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 should include user account name, the IP address, unsuccessful/successful attempts and time of occurrence. Covered entities must 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.

In order to monitor network activity, agencies should maintain logs of logon attempts to ascertain if there were unauthorized attempts to access servers. Typical operating systems are capable of logging user account names, their IP addresses, and the time of access attempts. Logon attempt logs are a valuable source of information should an unauthorized attempt be discovered.

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.

Level C data is considered to be very sensitive and Level D data is considered to be extremely sensitive by the Data and System Security Classification standard and must be protected when sent outside an agency. In order to protect the information, external recipients must sign a nondisclosure agreement or agencies must redact, or remove from view, the very sensitive and extremely sensitive data elements. In some cases, data considered sensitive may be sent to another entity for verification purposes, such as sending the entity an address for verification.

5.2.1 User Account Management

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

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

It is important to deactivate accounts when users are no longer employed or when a user's role changes in the agency. Procedures should be created to ensure that user accounts exist only for those that are active users.

5.2.2 Violation and Security Activity Reports

5.2.2.1 Information technology security administrators should 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.

It is important to log and report significant violation and security activity appropriately. Agency management is ultimately responsible for an agency's resources and violations should be reported. Agency information technology personnel need to know about security violations so they can take appropriate action to stop the activity and minimize the damage. The State Security Office keeps track of security activity to identify trends. In cases where prosecution or further investigation is likely, law enforcement officials must be notified.

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.

The State Security Office is the focal point for cybersecurity information throughout state government and can offer assistance to state agencies and other public organizations.

5.2.3 Firewalls

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

Firewalls are a good way to filter out all network traffic that is clearly invasive and threatening. Combining different types of firewalls makes an organization harder to compromise. There are many different types of firewalls that are hardware or software-based that protect servers and desktops.

Tips for Effective Physical Security

- Keep a log of all individuals admitted to secured areas.
- Sufficient measures should be put in place and maintained for protection against environmental factors (i.e., fire, dust, power, excessive heat and humidity).
- Generators to provide power in the event of an electrical interruption are desirable.
- Have formal, documented policies and procedures that govern the receipt and removal of hardware/software from a facility.
- Document repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks.
- Use surge protectors when possible on all machines.
- Physical security includes the end user machines. Make provisions for individual workstations by locking them with a password-protected screensaver when the user is away from the workstation.
- Laptops, PDAs, and other mobile computing devices should be protected during transport by placing in secured storage or having them in your possession.
- When possible, users should lock their workstations any time they leave their immediate work area.

Critical Resources

Data centers, wiring closets and other rooms with critical resources ideally:

- Should have access restricted to those authorized because of a need for access
- Should have locked doors even during normal business hours
- Should have adequate electric wiring with proper grounding
- Should be located in areas that are not subject to flooding
- Should not have windows to the outdoors
- Should be protected with non-water-based fire suppression systems
- Should be in a location as obscure to the public as practical
- Should not overtly advertise their location (i.e., listings on boards in public areas)
- When not staffed, should be monitored with a system to provide notification in case of heat, moisture, or access outside of set parameters
- Should not contain unnecessary flammable materials such as cardboard boxes and extra paper
- Should provide closed cabinets for needed flammable materials such as log books and manuals
- Should not contain dust producing devices such as paper shredders or high speed printers
- Should assure proper disposal of physical data records, including computers and their components, removable media (i.e. tape, diskettes, CDs), printouts, and microfiche

For more information about effective security practices, contact:

State Security Office
(501) 682-4300
http://www.cio.arkansas.gov/security