STATE OF ALABAMA

Information Technology Policy

POLICY 651-01: PHYSICAL SECURITY

Physical security controls are implemented to protect information system resources, the facility housing those resources, and the facilities used to support their operation. To protect against loss of control over system integrity and system availability, organizations need to address physical access controls, environmental controls, fire safety, and protect systems and data storage media from theft.

OBJECTIVE:

This policy communicates the essential aspects of physical security of computing equipment and data storage media that must be practiced by all information technology organizations to safeguard the integrity and availability of State information system resources and data.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

- Ensure computer systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Ensure laptop and portable computers are secured with an appropriate physical security device such as a lockdown cable. Computer equipment installed in public areas shall be similarly secured.
- Control access to areas containing servers, data stores, and communications equipment. Access to secured areas shall be controlled by the use of access card keys, access code keypads, or key locks with limited key distribution. A record shall be maintained of all personnel who have authorized access.
- Closely control keys (where utilized). If a key is reported as missing, change or re-key the corresponding lock(s).
- Change access codes, where utilized, at least every 90 days or immediately upon removing someone from the authorized access list.
- Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months.
- Ensure visitors are escorted by a person with authorized access to the secured area.
- Ensure each facility containing computer and communications equipment has an appropriate fire suppression system and/or a class C fire extinguisher readily available and in working order.
- Store equipment above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness or flooding. Use of water/moisture sensors is recommended.
- Monitor and maintain data center temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.

- Store electronic media in secured and environmentally controlled areas, in fire safe containers whenever feasible. Backup/archive media shall, whenever feasible, be stored in a secure off-site storage facility.
- Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location.
- Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

SUPPORTING DOCUMENTS:
- Information Technology Procedure 681P1: Equipment Disposal
- Information Technology Standard 681S3: Media Sanitization

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
651-00	05/31/2011	Combines and replaces Policy 650-01 and Standard 650-01S1; added temperature and humidity control requirement.
651-01	02/28/2012	Added equipment delivery and removal control, links to Equipment Disposal Procedure and Media Sanitization Standard; rephrased several statements.