# STATE OF ALABAMA

## Information Technology Standard

# STANDARD 681S1-00: INFORMATION PROTECTION

The cornerstone of information security is protecting data from unauthorized disclosure (confidentiality), unauthorized modification or destruction (integrity), and preventing disruption of access to or use of information systems (availability).

Information and information systems security categorization standards provide a common reference for expressing information protection requirements, effective management of security programs, and consistent reporting of the adequacy and effectiveness of security policies, standards, and procedures. In the course of conducting State business, personnel may have access to highly sensitive data and information systems. Personnel must understand how information and information systems are categorized and what protection measures are required to ensure the confidentiality, integrity, and availability of information.

### OBJECTIVE:

Establish the basis for assigning an appropriate level of security to the retention, transmission and handling of State of Alabama information in accordance with State IT Policy 681: Information Protection.

### SCOPE:

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

### REQUIREMENTS:

Information covered by these requirements includes, but is not limited to, information that is either transmitted or stored (including hard copy and all electronic information, information transmitted via facsimile, instant message, e-mail, e-mail attachment, and the transfer of information via public networks).

## INFORMATION PROTECTION CATEGORIES

All State information and information systems shall be assessed and identified as belonging in one of the following four categories:

**PUBLIC**: Information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the State or to any individual. Disclosure of public information should be expected to have no adverse effect on State operations, State assets, or individuals.

**INTERNAL**: Information intended primarily for employees of the State (personnel information, descriptions of work processes, information technology standards and procedures, etc.) shall be limited to internal distribution. The unauthorized disclosure of internal information could be expected to have a **limited** adverse effect on State operations, State assets, or individuals.

**SENSITIVE**: Sensitive information includes (but is not limited to) personally identifying information (such as that specified in State Statute 41-13-7 which includes date of birth, social security number, driver's license number, etc.), and other personal information that could undermine individual integrity (personnel records, disciplinary action records, etc.). This category also includes Protected Health Information (PHI) as defined by the Health Information Portability and Accounting Act (HIPAA) of 1996 or Federal and State regulations. The unauthorized disclosure of

sensitive information could be expected to have a **serious** adverse effect on State operations, State assets, or individuals.

**CONFIDENTIAL**: Information that must be protected to ensure the security of State residents and resources. Confidential information may include data pertaining to State infrastructure (utilities and services), records of legal proceedings, and data protected as evidence. The unauthorized disclosure of confidential information could be expected to have a **severe or catastrophic** adverse effect on State operations, State assets, or individuals.

Information belonging or pertaining to another organization that has been entrusted to the State by that organization under non-disclosure agreement or contract may be categorized "Third Party Sensitive" or "Third Party Confidential."

Additional information protection categories may be defined and used at agency discretion; however, the aforementioned categories shall not be modified nor used in a manner that reduces the required protections defined by this standard.

## INFORMATION PROTECTION REQUIREMENTS

The requirements defined in the information protection matrix (table on next page) provide details on how to protect information based on its protection category. Use this as a reference when determining how to handle data. More stringent measures of protection may be required depending upon the circumstances and the nature of the information in question.

Organizations shall document information protection procedures specific to their operational practices and information protection requirements that implement and comply with these and other applicable State standards.

### ADDITIONAL INFORMATION:

Information Technology Policy 681: Information Protection
http://cybersecurity.alabama.gov/documents/Policy_681_Information_Protection.pdf

Information Technology Standard 681S2: Protecting Personally Identifiable Information
http://cybersecurity.alabama.gov/documents/Standard_681S2_Protecting_PII.pdf

Information Technology Standard 681S3: Media Sanitization
http://cybersecurity.alabama.gov/documents/Standard_681S3_Media_Sanitization.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

*By Authority of the Office of IT Planning, Standards, and Compliance*

### DOCUMENT HISTORY:

| Version | Release Date | Comments |
|---|---|---|
| 680-01S1 | 5/23/2006 | Original document |
| 680-01S1_A | 9/5/2007 | Require access controls for sensitive data |
| 680-01S1_B | 7/12/2010 | Modified Sensitive data definition. |
| 681S1-00 | 09/01/2011 | Document number and format change only |
| | | |

**Table: Information Protection Matrix**

| CONTROL▶ | Access | Marking | Distribution | | | Storage | Disposal |
|---|---|---|---|---|---|---|---|
| CATEGORY▼ | | | Internal | External | Electronic | | |
| **Public** | Anyone | None | Any means | Any means | Any means | No restriction | Any means |
| **Internal** | State employees and vendors with a need to know. | "State Use Only" or "[Agency] Use Only" | Standard interoffice mail, approved e-mail, Instant Message, or other approved electronic distribution methods. | US Mail or other public or private carrier, approved e-mail, and other approved electronic distribution methods. | Send only to approved recipients | Protect from view or loss; use individual access controls when possible. | Reliably erase or physically destroy all storage media when data is no longer required. |
| **Sensitive** | State employees with a need to know.<br><br>Vendors with signed non-disclosure agreement. | "Sensitive" or "[Third-party] Sensitive "<br><br>Protect printed materials with cover sheet. | Standard interoffice mail, approved e-mail, or approved electronic distribution methods. | US Mail or approved private carrier. | No restriction when sent to approved recipients within State network.<br><br>Outside State network send via private link and/or encrypt. | Use Individual access controls.<br><br>Encrypt stored electronic data when possible.<br><br>Do not store on personally-owned systems/media. | Reliably erase or physically destroy all storage media when data is no longer required. |
| **Confidential** | State employees with specific access approval and documented need to know.<br><br>Vendors with signed non-disclosure agreement. | "Confidential" or "[Third-party] Confidential"<br><br>Control or tracking numbers when utilized.<br><br>Protect printed materials with cover sheet. | Delivered direct - signature required, or approved electronic distribution methods. | Approved private carrier; delivered direct - signature required. | Encrypted; receipt requested. | Use individual access controls, all access logged, and appropriate audit trails created and retained.<br><br>Encrypt stored electronic data; physically secure all other data forms.<br><br>Do not store on personally-owned systems/media. | Reliably erase or physically destroy all storage media when data is no longer required.<br><br>Retain audit trail indicating when and by whom data was disposed. |