# STATE OF ALABAMA

## Information Technology Policy

## POLICY 685-00: DATA BREACH NOTIFICATION

State government agencies are committed to protecting the privacy of Alabama citizens. Each organization must implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive personal information when the unauthorized use of such information is likely to result in substantial harm or inconvenience to the individual to whom the information relates.

For the purposes of this policy, a data breach (or breach of data security) is the unauthorized acquisition, access, use, or disclosure of sensitive personal information, data that specifically identifies a person or a person's property and compromises the security or privacy of that individual.

Such identifying information may include any of the following information related to a person:

- Date of birth
- Social Security number
- Driver's license number
- Financial services account numbers, including checking and savings accounts
- Credit or debit card numbers
- Personal identification numbers (PIN)
- Electronic identification codes
- Automated or electronic signatures
- Biometric data
- Fingerprints
- Passwords
- Parents' legal surname prior to marriage
- Home address or phone number
- Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services

Identifying information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

This policy defines the reporting requirements in the event of a breach of identifying information.

### OBJECTIVE:

To protect data relating to citizens and to require notification of data security breaches.

### 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:

Unless overridden by statutory or regulatory obligations (such as HIPAA) the following requirements apply when the privacy or confidentiality of sensitive personal information has been compromised.

## Agency Management, Information Technology Organization:

Notify affected individuals following the discovery of a data breach.

Notification is NOT required when the breached data is in a form that is unusable, unreadable, or indecipherable to unauthorized individuals; meaning data that is either encrypted or destroyed in accordance with State policies and standards.

- Acceptable encryption technologies are described in State IT Policy 683: Encryption
- Acceptable destruction methods are described in State IT Standard 681S3: Media Sanitization

Notification is also NOT required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the agency reasonably determines that the breach has not and likely will not result in harm to the individuals whose personal information has been acquired and accessed. Such a determination shall be documented in writing and the documentation shall be retained for 5 years.

## Data Owner/Data Custodian:

In the event of a data breach, where notifications are required, the Data Owner is responsible for notifying affected individuals. The Data Owner is the data originator or primary entity responsible for the data use (processing) or disclosure.

In a custodial arrangement, where the data storage and/or transmission media is provided by a third party that is not the Data Owner, in the event of a data breach where notifications are required the Data Custodian (the entity responsible for the system(s) on which the data is stored and/or transmitted) shall notify the Data Owner. The Data Custodian shall (if possible) identify for the Data Owner the individuals whose data has been, or is reasonably believed to have been, breached.

## ADDITIONAL REQUIREMENTS:

## Notification Methods:

Notification may be provided by one or more of the following methods:

- Written notice;
- Electronic notice (provided the entity providing the notice has a valid e-mail address for the subject person and the subject person has agreed to accept communications electronically);
- Conspicuous posting of the notice on the web page of the person (if the person maintains a web page);
- Notification to major statewide or broadcast media;
- In accordance with the agency's policies or the rules, regulations, procedures, or guidelines; or
- Pursuant to the rules, regulations, procedures, or guidelines established by the agency's primary or functional federal regulator.

## Notification Time Limits:

Notifications to affected individuals shall be made without unreasonable delay but not later than 60 calendar days after discovery of a breach.

Data Custodians shall notify Data Owners as soon as possible but not later than 10 calendar days following the discovery of a data breach.

Notifications may be delayed when a law enforcement official determines that notification would impede a criminal investigation or cause damage to national security.

## SUPPORTING DOCUMENTS:

- Information Technology Standard 681S3: Media Sanitization
- Information Technology Policy 683: Encryption

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

## DOCUMENT HISTORY:

| Version | Release Date | Comments |
|---|---|---|
| 685-00 | 01/18/2012 | Original document |
| | | |
| | | |