STATE OF ALABAMA

INFORMATION TECHNOLOGY POLICY

Policy 621: Data Breach Notification		
Document/Version: 621-01	Version Date: 07/10/2020 (draft)	Effective Date: TBD

OBJECTIVE

The objective of this policy is to define the requirements and responsibilities for providing notifications when a breach of personal information has occurred.

STATEMENT OF POLICY

State government is committed to protecting the privacy of Alabama citizens. The Alabama Data Breach Notification Act of 2018 (***Chapter 38 of Title 8, Code of Alabama 1975; Act 2018-396***) requires certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information (PII).

This policy supports implementation of the Alabama Data Breach Notification Act and expands the provisions and requirements of the Act as follows. This policy does not replace the Act or any other law or industry standard regarding breach notification.

It is the policy of OIT that:

a) The definition of a BREACH OF SECURITY or BREACH as defined in the Act includes the unauthorized acquisition of data in electronic form containing sensitive personally identifying information (PII), [*Acts 2018-396*], and shall be further construed to include:

(1) the unauthorized <u>use</u> or <u>disclosure</u> of data in electronic form containing sensitive PII, and

(2) information spillage instances where sensitive PII is inadvertently placed on information systems that are not authorized to process such information. [*IRS 1075, IR-9*]

b) PERSONALLY IDENTIFYING INFORMATION (PII) is defined as an Alabama resident's first and last name or first initial and last name in combination with one or more of the following:

(1) A non-truncated Social Security number or tax identification number.

DRAFT

(2) A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.

(3) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.

(4) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. This may also be referred to as Protected Health Information or PHI.

(5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual (also PHI).

(6) A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information. [(1)-(6): *Act 2018-396*]

(7) PII may also include:

- Date of birth
- Automated or electronic signatures
- Biometric data
- Fingerprints
- Passwords
- Parents' legal surname prior to marriage
- 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.

[*Alabama Consumer Identity Protection Act* (*Act 2001-312*)]

c) PII does not include information about an individual which has been made public by a federal, state, or local government record or widely distributed media. [*Act 2018-396*]

DRAFT

d) The term SUBSTANTIAL HARM shall be construed to mean a serious adverse effect on individuals which may result in:

(1) significant financial loss,

(2) significant physical harm or injury, or

(3) loss of the privacy to which individuals are entitled under law. [*FIPS 199*]

OIT RESPONSIBILITIES

As an IT service provider, OIT acts as a Data Custodian. Other service providers (vendors) may also act as data custodians and shall be required to adhere to the following responsibilities.

Data Custodians shall:

O.1 Immediately notify the affected agency (the Data Owner) when a data breach has been detected.

O.2 Have documented procedures for notifying agencies in the event of a breach of agency data from host systems.

O.3 Assist agencies with detection, response, and recovery efforts following a breach of security.

AGENCY RESPONSIBILITIES

Data ownership typically resides at the agency level. Agencies may also be stewards of and responsible for data provided by (and ultimately owned by) a federal source (e.g., Federal Tax Information or FTI).

Agencies or Data Owners shall:

A.1 Notify, in accordance with applicable law, regulations, rules, or policies, the individuals affected by a data breach.

A.2 Notify the OIT Security Operations Center (SOC) upon discovery of any data breach. Notification to the OIT SOC shall occur as soon as practical after discovery of the breach and, if practical, before any significant actions are taken on affected systems.

USER RESPONSIBILITIES

Information system users shall:

U.1 Immediately inform their supervisor or Senior Agency Information Security Officer (SAISO) upon discovering that a data breach may have occurred regardless of its perceived impact to individuals or to agency operations.

DRAFT

U.2 SAISOs should, as soon as practical, notify the OIT SOC. SOC personnel can assist with detection, response, and recovery efforts.

SUPPORTING DOCUMENTS

The following documents support this policy:

- Policy 620: Cyber Incident Response

The following special publication (SP) of the National Institute of Standards and Technology (NIST) supports this policy and may aid in its implementation:

- NIST SP 800-61: Computer Security Incident Handling Guide

AUTHORITY

This policy is promulgated under the authority of the Office of Information Technology (OIT) as described in Policy 101: IT Governance.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
685-00	01/18/2012	Original version (Rescinded June 2018)
621-01	07/10/2020	DRAFT; completely revised from original version

DRAFT