ITS Data Breach Notification Policy
Notice of Approval

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3005	
	Title: ITS Data Breach Notification Policy	
	Document Type: ITS Agency	
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 09-25-2017	**Revision Date:** 09-25-2017

Notice is hereby given, that the above specified document meets the requirements of the Mississippi Department of Information Technology Services Policies, Standards and Guidelines Program, defined in ESW-PSG-1001, thereby warranting approval for implementation, effective immediately.

Executive Director
Mississippi Department of
Information Technology Services

September 25, 2017
Date of Signature

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3005	
	Title: ITS Data Breach Notification Policy	
	Document Type: ITS Agency	**Page:** 1 of 5
	Domain: Security | Compliance	**Status:** Pending Approval
	Effective Date: 09-25-2017	**Revision Date:** 09-25-2017

1. AUTHORITY

The Mississippi Department of Information Technology Services (ITS) shall issue recommended strategies and goals for the effective and efficient use of information technology and services in state government (§ 25-53-29(2)). Additionally, ITS shall publish written planning guides, policies and procedures for use by agencies and institutions in planning future electronic information service systems (§ 25-53-29(1) (b)).

2. PURPOSE

The Data Breach Notification Policy provides guidance to the Mississippi Department of Information Technology Services (ITS) concerning the steps to notify impacted entities in the event of a discovered data breach. ITS is committed to protecting the electronic files, media, databases and data maintained within the State Data Centers. ITS must implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive information from the unauthorized use of such information which will likely result in substantial harm or inconvenience to the State.

3. SCOPE

The Data Breach Notification Policy applies to all ITS staff defined as full-time, part-time, temporary, or contract employee who are authorized to use agency information systems.

The Data Breach Notification Policy does not include publicly available information that is lawfully made available to the public from federal, state, or local government records or widely distributed media.

The Data Breach Notification Policy is a complimentary document to the Cyber Security Incident Reporting Guide for the interaction within and between ITS, the Information Security Division, and state agencies in the event of a data breach.

4. POLICY

The State of Mississippi, Information Technology Services, shall have effective data breach notification procedures that ensure appropriate steps are taken to report a breach of sensitive data. The data breach notification procedures shall compliment the Enterprise Information Security Policy in protecting the confidentiality and security of sensitive information when the unauthorized use of such information is likely to result in substantial harm or inconvenience to the State.

5. STANDARDS

5.1 ITS staff that become aware of a data breach or suspects a data breach of sensitive data shall immediately report the incident to the Chief Operations Officer and their supervisor.

5.2 The ITS Chief Operations Officer shall appoint a Data Breach Advisory Team to review any real or suspected data breach. The Data Breach Advisory Team and Chief Operations Officer shall provide appropriate escalation and notification in the event of an actual data breach.

5.3 A Public Information Officer shall notify the affected entities of the incident in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system of all incidents. The owner of the personal information should be notified as soon as practicable following the breach discovery (Mississippi HB 583).

6. GUIDELINES

6.1 Notification Methods

6.1.1 In the event of an actual data breach where notifications are required. Notification may be provided by one or more of the following methods:

6.1.2 Written notice;

6.1.2.1 Electronic notice (provided the entity providing the notice has a valid e-mail address for the subject entity and the subject entity has agreed to accept communications electronically)

6.1.2.2 Conspicuous posting of the notice on the web page of the entity

6.1.2.3 Notification to major statewide or broadcast media

6.1.2.3.1 In accordance with the agency's policies or the rules, regulations, procedures, or guidelines; or

6.1.2.3.2 Pursuant to the rules, regulations, procedures, or guidelines established by the agency's primary or functional federal regulator.

6.2 Agency partners should notify ITS Chief Operations Officer if the Agency becomes aware of a security incident that potentially affects Agency systems or data hosted in the state data centers.

6.3 Sensitive data refers to privileged or proprietary information that only certain people are allowed to see and is therefore not accessible to everyone. If sensitive data is lost or used in any way other than intended, the result can be severe damage to the people or organization to which

that information belongs.

7. ATTACHMENT

Example of Sensitive Data

8. REFERENCES

§ 25-53-29 (2)
§ 25-53-29 (1) (b)
Mississippi HB 583

Examples of Sensitive Data

ITS may not be aware of all sensitive information maintained by Agency Partners within the ITS Data Center. Therefore, the following are some common types of sensitive, protected data. The intent of this list is a guideline and not as a complete list of sensitive data.

Credit Card or Payment Card Industry (PCI) Information

Information related to credit, debit, or other payment cards. This data type is governed by the Payment Card Industry (PCI) Data Security Standards. Credit or debit card numbers cannot be stored in any electronic format.

Federal Information Security Management Act (FISMA) Data

The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document, and implement security programs for information technology systems and store the data on U.S. soil.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is a category of sensitive information that is associated with an individual person. PII should be accessed only on a strict need-to-know basis and handled and stored with care.

PII is information that can be used to uniquely identify, contact, or locate a single person. Personal information that is “de-identified” (maintained in a way that does not allow association with a specific person) is not considered sensitive.

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

Protected Health Information (HIPAA)

Protected Health Information (PHI) is defined by the Health Insurance Portability and Accountability Act (HIPAA). PHI is individually identifiable health information that relates to the

- Past, present, or future physical or mental health or condition of an individual.
- Provision of health care to the individual by a covered entity (for example, hospital or doctor).
- Past, present, or future payment for the provision of health care to the individual.

Social Security Numbers

Social Security numbers are unique, nine-digit numbers issued to U.S. citizens, permanent residents, and temporary (working) residents for taxation, social benefits, and other purposes. Social Security numbers are a primary target for identity thieves. They fall into the U-M category of sensitive Personally Identifiable Information (PII). U-M

has not used Social Security numbers as identifiers for students and employees since 2004.

Student Education Records (FERPA)

Records that contain information directly related to a student. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records.

Student Loan Application Information (GLBA)

Personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. Gramm Leach Bliley Act (GLBA) provisions govern this data type.