OFFICE OF CHIEF INFORMATION OFFICER
Summary of the State Board of Education Agenda Items
Consent Agenda
April 19, 2023

OFFICE OF TECHNOLOGY AND STRATEGIC SERVICES

T. Approval to begin the Administrative Procedures Act process: To establish Miss. Admin. Code 7-3: Chapter 55, Rule 55.2: Data Classification Policy

Background Information: Under Miss. Admin. Code 7-3: 55.1, State Board Policy, Chapter 55, Rule 55.1, the Mississippi Department of Education (MDE) Office of Technology and Strategic Services (OTSS) established – and supports – the agency-wide Data Governance program, implemented through the Data Governance Committee (DGC). The DGC develops and promulgates processes, as well as rules and regulations governing the data that apply to all program offices within the MDE.

The proposed new rule establishes a new data classification policy for MDE. This policy will serve as a framework to guide the DGC as it makes determinations regarding student and school/district personnel data to ensure that all data is properly stored, maintained, and disseminated. Under the authority reflected in the Data Governance Charter – and in compliance with state and federal laws – the DGC will guide OTSS as it implements the data classification policy through all data systems, processes, and procedures.

Recommendation: Approval

Back-up material attached

Chapter 55: Information and Operational Technology
Rule 55.2 Data Classification Policy

Under Miss. Admin. Code 7-3: 55.1, State Board Policy, Chapter 55, Rule 55.1, the Mississippi Department of Education (MDE) Office of Technology and Strategic Services (OTSS) established – and supports – the agency-wide Data Governance program, implemented through the Data Governance Committee (DGC). The DGC develops and promulgates processes, as well as rules and regulations governing the data that apply to all program offices within the MDE.
To protect the privacy of students and school/district personnel, and ensure that all data is properly stored, maintained, and disseminated, the following **Data Classification Policy** shall be implemented through all data systems, processes, and procedures under the supervision of the DGC, under the authority reflected in the Data Governance Charter.

1. Roles and Responsibilities

A. The Data Governance Committee shall review the Data Governance Charter and the Data Governance Procedure Manual to ensure that the responsibilities of key roles – including the Data Governance Manager, Data Owners, and Data Technicians – appropriately address the established data classification policy.

B. The Data Governance Committee shall advise OTSS how the implementation of the data classification policy impact end users to ensure their level of access and acknowledgement of their data privacy obligations and aligned to the data they access and use.

C. The Data User is the person, organization or entity that interacts with, accesses, uses, or updates data for the purpose of performing an authorized task. Data Users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to data use.

2. Levels of Classification

The DGC establishes three (3) categories for data classification according to their sensitivity and importance to the functional compliance with state and federal laws, and policies, under which all data will be classified:

A. **Public Data**: Public (or Low Risk) Data is defined as information with no existing local or national legal restrictions on access or usage. Public data includes information that may be or currently is released to the public. It does not require protection from unauthorized disclosure. This information is available to the public, and illustrative (but non exhaustive) examples to show the nature of this data include:
   i. posted programs and services;
   ii. information regarding institution and facility characteristics;
   iii. announcements, advertisements, district and school contact information, and other freely available data.

B. **Protected Data**: Protected (or Moderate Risk) Data may not be specifically protected from disclosure by law but cannot be released in combination with any identifying information such as student identifiers or demographic data. Protected information is generally not released to the public unless requested and must be de-identified in compliance with state and federal laws. The FERPA standard for de-identification assesses whether a "reasonable person in the school community who does not have personal knowledge of the relevant circumstances" could identify individual students based on reasonably available information, including other public information released by an agency, such as a report presenting detailed data in tables with small size cells (34 CFR §99.3 and §99.31(b)(1)). Illustrative examples of de-identified data to show the nature of protected data include:
   i. de-identified individual assessment results;
   ii. de-identified individual attendance records;
   iii. de-identified individual course selection and enrollment data for students.

C. **Sensitive Data**: Sensitive (or High-Risk) Data is considered confidential, privileged, or personal information protected by statutes, regulations, state and federal policies or contractual language (FERPA, PPRA, IDEA, etc.). Sensitive information includes Personally Identifiable Information (PII). Exposure or breach could result in liability issues, fines/penalties, identify theft and/or financial fraud. Sensitive information is specifically protected from disclosure by law. It may include, but is not limited to:
   i. Personal information about individuals, regardless of how that information is obtained;
   ii. Unique identifiers, including Social Security Numbers;
   iii. Information concerning employee personnel records;
   iv. Information regarding IT infrastructure and security of computer and telecommunications systems;
   v. Individual Student National School Lunch Status.

D. Data compiled from multiple sources is to be classified with the most secure classification level designation of any individually classified data or source.

References: Miss. Code Ann. §§ 25-53-1 through 25-53-25, § 25-53-201, § 25-61-1 et seq., § 37-1-3, § 37-3-5, § 37-151-9, § 75-24-29 et seq., MS ITS Enterprise Security Policy Miss. Admin. Code 36: 1 et seq., Every Student Succeeds Act (ESSA), Individuals with Disabilities Education Act (IDEA), Family Educational Rights and Privacy Act (FERPA), Richard B. Russell National School Lunch Act (NSLA), Children's Online Privacy Protection Act (COPPA), Protection of Pupil Rights Amendment (PPRA), Children's Internet Protection Act (CIPA), Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards Technology (NIST), Federal Information Processing Standards 200 (FIPS)