OFFICE OF CHIEF INFORMATION OFFICER
Summary of the State Board of Education Agenda Items
Consent Agenda
January 16, 2020

OFFICE OF TECHNOLOGY AND STRATEGIC SERVICES

G. Approval to begin the Administrative Procedures Act process: To revise Miss. Admin. Code 7-3:55.1, State Board Policy Chapter 55, Rule 55.1

The proposed revision will provide guidance to the MDE and Local Educational Agencies regarding the Office of Technology and Strategic Services operational responsibilities as it relates to Data Governance, Security, and Privacy.

Recommendation: Approval

Back-up material attached

Chapter 55: ~~Technology and Strategic Services~~

Rule 55.1 Technology and Strategic Services

1. ~~The Office of Technology and Strategic Services (OTSS) is to ensure appropriate authorized access of IT resources and services, equipment and usage for the security and protection of information as assigned by State of Mississippi. These resources are provided to conduct and support state business and educational functions as required by law. OTSS provides security and controls to enhance efforts in providing confidentiality, integrity and availability to the departments within MDE as with student and personnel information in schools, public and nonpublic school districts governed by the State Board of Education. All information technology assets that are managed, operated, maintained, or in the custody or proprietorship of the agency and/or hosted by third parties on behalf of MDE must be utilized to ensure:~~

   a. ~~Appropriate Use~~
   b. ~~Availability~~
   c. ~~Accountability~~
   d. ~~Data Integrity~~
   e. ~~Privacy and Confidentiality~~

   ~~Employees and authorized users are required to adhere to the "Appropriate and Acceptable Use Policy" that is published in the MDE Human Resource Employee Policy and Procedures Manual and on the OTSS website. Users must read and acknowledge the policy as a condition of being granted access to Office of Technology and Strategic Services' technology assets during their tenure as an employee or authorized user. Users will be held responsible for protection of all technology resources and information for which they are entrusted and using them for their intended purposes.~~
   ~~The Office of Technology and Strategic Services Security Policy has been created as a directive of MS Information Technology Services as it applies in MS Code 25-53-1 to §25-53-25. Each agency must establish a framework to operate, develop, implement and apply appropriate security measures to protect and safeguard the agency and its users from forms of unauthorized access, malicious misuse, disclosure, modification or inadvertent compromise.~~

   ~~State board governed schools, public and non-public school districts are required to create a district wide Information Technology Security Policy. The policy will develop, implement and maintain district information technology resources that are managed, operated or in the custody or proprietorship of the district and/or MDE and/or hosted by third parties on behalf of the school district and/or MDE. The requirements and standards cannot be less than those established in the OTSS Information Technology Security Policy.~~

   ~~The more restrictive policy will take precedence in the event of a conflict between the agency's policy and the district's policy.~~

2. ~~Information Technology Steering Committee (ITSC)~~

~~The Information Technology Steering Committee is established to be the coordinating body for the agency and school districts technology resources and information security- related activities. It is composed of appointed staff from the Office of Technology and Strategic Services and~~

~~representatives appointed by the State Superintendent of Education and/or a Deputy Superintendent of Education.~~

~~3. ITSC responsibilities include:~~
~~Assisting the Chief Information Officer (CIO) in developing, reviewing, and recommending technology resources and information security policies for the agency and all governed school districts by the board~~
~~Identifying and recommending industry best practices for technology asset usage and information security~~
~~Developing, reviewing, implementing and recommending federal and statewide standards, procedures and guidelines~~
~~Coordinating inter-departmental and school district professional and accurate communication and collaboration on technology usage, security issues and future access system changes~~
~~Coordinating statewide information technology and security education and awareness to all governed school districts by the state board~~

Source: *Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards Technology (NIST), Federal Information Processing Standards 200 (FIPS)*
The Family Educational Rights and Privacy Act (FERPA) ~~*(20 U.S.C. §1232g; 34 CFR Part 99) No Child Left Behind Act of 2001, The*~~ *Individuals with Disabilities Education* ~~*Improvement*~~ *Act* ~~*of 2004*~~ *(IDEA)*~~*34CFR 300.560-300.577, The U.S. Department of Agriculture – Use of Free and Reduced Price Meal, Eligibility Information Nondiscrimination or Identification of Recipients, 42USC 1758 (b)(2)(C)(iii),*~~ *Richard B Russell National School Lunch Act* ~~*(42U.S.C. 1751 et seq.) The Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.),*~~
Miss. Code Ann. §37-1-3, 37-3-5, §37-151-9, §25-53-1 to §25-53-25 ~~*(Revised 4/2016)*~~

Chapter 55: Information and Operational Technology
Rule 55.1 Office of Technology and Strategic Services

The Office of Technology and Strategic Services (OTSS) is to support the strategic mission and vision of the State Board of Education (SBE). To accomplish the support of the strategic mission and vision, OTSS will implement and support sound governance, a secure and stable infrastructure, reliable systems and applications, and timely and quality data controlled within the Mississippi Department of Education (MDE). The MDE is committed to compliance with federal and state laws regarding data security and privacy.

1. With regard to OTSS's broad, operational responsibilities, the SBE charges OTSS with:

    a. Validating and managing data, documenting and managing data definitions, establishing and supporting workflow processes, and implementing and managing business rules established through data governance and state/federal law for all data submitted to or collected by the MDE;
    b. Managing all information technology resources, including physical, virtual, and cloud;
    c. Ensuring the availability and integrity of systems and applications managed by the MDE;
    d. Securing networks, systems, and data, including monitoring and mitigating against threats;
    e. Granting access to information technology systems, applications, data, and reports to appropriate users;
    f. Managing databases and data flows, analyzing data, and generating reports;
    g. Adhering to information technology best practices, and state/federal mandates and guidelines regarding the collection, storage, and disclosure of personally identifiable information (PII) of students, educators, parents, and MDE personnel.

2. With regard to OTSS's specific responsibilities related to security, privacy and governance, the SBE charges OTSS with:

    a. Staffing OTSS leadership positions with specific security, privacy and governance responsibilities;
    b. Establishing and supporting an agency-wide Data Governance Program;
    c. Developing, administering and ensuring compliance with policies and procedures necessary to ensure security and privacy (*See* Section 6);
    d. Monitoring, managing and mitigating security and privacy risks;
    e. Providing mandatory security, privacy and governance training to all MDE personnel
    f. Regularly reporting on the security and privacy posture and status of the MDE to the State Superintendent of Public Education;
    g. Sharing with public school districts information technology best practices, and state/federal mandates and guidelines regarding the collection, storage, and disclosure of personally identifiable information (PII) of students, educators, parents, and MDE personnel.

3. The following terms shall have the meanings ascribed to them in this section unless the context otherwise requires:
    a. “Authorized User” is a consumer of information technology and data that has been entrusted access based on the Principal of Least Privilege to perform a function for the MDE.
    b. “Building consensus” is the mediation of a conflict involving many parties.
    c. “Business Analyst” is a person who performs analysis of an information system’s requirements, functions, and interdependencies.
    d. “Change Management” is the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.
    e. “Data” is the raw un-synthesized facts and statistics collected for reference or analysis.
    f. “Data Steward” is the program office designee responsible for determining how data are defined, collected, audited, and reported to meet the program office and agency requirements.
    g. “Escalating issues” is the act of bringing an item that has stalled in the resolution process to the attention of person(s) who has the ability to direct a resolution path.
    h. “Governance” is the agency-wide structure and processes for collaborative decision-making and management of the MDE data assets to improve quality and use, while enhancing security and privacy protections.
    i. “Incident” is an occurrence that potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
    j. “Information” results from data processing that has become useful for analysis.
    k. “Information Technology” are systems for creating, consuming, transmitting, and/or storing data and information .
    l. “Local Education Agency (LEA)” are school districts within the state governed by the MDE.
    m. “Mitigation” is the action of reducing the severity, seriousness, or damaging effects of a risk or incident.
    n. “The Principal of Least Privilege (POLP)” is providing access limited to the minimum rights and permissions an authorized user requires to perform their assigned function.
    o. “Personally, Identifiable Information (PII)” is any information or data that could used or be combined to positively identify an individual (e.g., name, address, SSN)
    p. “Risk” is a measure of the extent to which an entity is threatened by a potential circumstance or event.
    q. “Systems” are a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information.
    r. “Threat” is any circumstance or event with the potential to adversely impact the MDE.

4. The OTSS leadership positions with specific security, privacy, and governance responsibilities:

    a. The MDE Chief Information Officer (CIO) will have leadership responsibility for – and shall be dedicated to – the daily management and long-range vision and strategies of OTSS. This employee shall be charged with the following responsibilities, including but not limited to:
        i. Ensuring OTSS' goals and strategies support and further the Goals of the SBE Strategic Plan;
        ii. Providing strategic leadership to the MDE's information technology and data endeavors;
        iii. Ensuring that OTSS is appropriately staffed with dedicated and qualified professionals to achieve the Goals of the SBE Strategic Plan;
        iv. Establishing and maintaining project management and change management over the information technology and data of the MDE;
        v. Establishing and supporting data governance within the MDE;
        vi. Serving as the signatory for all the MDE's purchases and contracts in relation to information technology, operational technology, and data;

    b. The OTSS Information Security and Data Privacy Officer (ISO) shall be charged with the following responsibilities, including, but not limited to:
        i. Ensuring the security and privacy of all data and information within the MDE, by implementing agency-wide policies for sustaining, enhancing, and protecting the privacy and confidentiality of the data;
        ii. Working with the Data Governance Committee to develop, administer and ensure compliance with policies and procedures necessary to ensure security and privacy (*See* Section 6);
        iii. Identifying risks and threats to the MDE's information systems and assist in remediation of these risks in coordination with other OTSS resources;
        iv. Investigating and reporting any complaints of privacy violations, data breaches and/or cyber-attacks under MDE's jurisdiction – as well as coordinating with the appropriate authorities – in accordance with the processes and procedures outlined in the MDE's Incident Response Policy (*See* Section 6);
        v. Monitoring, investigating, and reporting on issues and incidents related to data privacy, security, governance, training and compliance – with this rule and with other applicable data security and privacy laws – to the State Superintendent of Public Education and the CIO;

    c. The OTSS Data Governance Manager (DGM) shall be charged with the following responsibilities, including, but not limited to:
        i. Facilitating and coordinating the development, implementation, and maintenance of the MDE Data Governance Program (*See* Section 5) to promote data quality, availability, usability, security, and privacy;

ii. Supporting the Data Governance Committee chair, providing facilitation for and coordination among data governance members and workgroups;
iii. Communicating with internal and external data governance stakeholders – including building consensus, escalating issues, implementing resolutions, and anticipating agency data issues and needs;
iv. Coordinating with data stewards and business analysts to document and analyze data processes and business rules – including engaging with various stakeholders to ensure awareness, buy-in, and compliance with data quality, security and privacy processes, and business rules;
v. Coordinating the development and adoption of key data governance artifacts - including data governance charter, guidelines, and a data dictionary;
vi. Coordinating the development and adoption of key data policies and procedures (*See* Section 6);
vii. Coordinating with the OTSS project managers to ensure that the prioritized agenda and project plans for key data governance artifacts and data policies are included in an agency-wide project portfolio.

5. The OTSS shall establish and support the agency-wide Data Governance Program. This program shall be charged with the following responsibilities:

a. The MDE Data Governance Program shall be implemented through the Data Governance Committee (DGC), comprised of members representing program offices across the MDE. The work of the DGC shall be authorized through the Data Governance Charter, as approved by the State Superintendent of Public Education. The DGC shall develop and promulgate policies and processes – as well as rules and regulations – governing the data that shall apply to all program offices within the MDE.

b. The DGC shall establish policies and processes to ensure that data collected by the MDE are stored, maintained, and disseminated in a manner that protects the data integrity and security, as well as the privacy of individuals involved. This includes specifying which data may or may not be collected by the MDE, as well as oversight and responsibility for ensuring data accuracy and validity as defined in the Data Dictionary.
i. The MDE program offices shall provide proposed changes to data collection no later than 30 days after SINE DIE. Change requests submitted after the 30-day mark will be held over for the future change request season, unless otherwise approved by the State Superintendent of Public Education or his/her designee.
ii. The DGC shall review and vote on all proposed changes to data collection by or before the September committee meeting.
iii. The DGC shall publish the revised Data Dictionary, reflecting the approved changes to data collection, by December 1st in preparation for the upcoming school year.

iv. The DGC shall establish policies and processes to ensure that these annual deadlines are met.

6. The DGC shall coordinate with OTSS to develop and maintain the following internal policies, procedures, standards, and guidelines – in addition to any others as needed to meet agency needs. The adoption, revision, and repeal of these policies, procedures, standards, and guidelines may require the approval of the State Superintendent of Public Education or his/her designee.

    a. Access, Account Management, and Password Policy
    b. Annual State of Security, Privacy, and Data Governance Report for the State Superintendent of Public Education
    c. Best Practices Guidelines
    d. Data Classification Framework
    e. Data Collection, Quality and Matching Standards and Procedures
    f. Data Destruction Policy
    g. Data Dictionary and Standards
    h. Data Sharing and Public Request Procedure
    i. Disaster Recovery and Continuity Policy
    j. Email and Electronic Communications Policy
    k. Incident Response Policy
    l. Information Technology Security Policy
    m. LEA Security and Privacy Notification Procedures
    n. Mandatory Annual Training Program, including Security Awareness and FERPA Training
    o. Safe, Appropriate, and Acceptable Use Policy
    p. Security and Privacy Processes and Procedures
    q. Security and privacy Violation Reporting Procedure
    r. Security Assessment and Compliance Policy
    s. Separation of Duties Standards
    t. Student and Parent's Rights
    u. Systems Capacity Planning Policy
    v. Vendor and Third-Party Control Policy

7. The OTSS shall develop and support MDE staff compliance with all policies and procedures necessary to monitor, manage and mitigate security and privacy risks.

    The CIO and ISO shall provide mandatory annual security and privacy training, including, but not limited to, security awareness and FERPA Compliance, to all MDE employees.

    MDE employee access to the MDE information technology and data shall be dependent upon their compliance with training completion and adherence to security and privacy policies, procedures, standards, and guidelines. Those who fail to complete this training or to adhere to the security and awareness program may be referred to ELT for termination of systems and network access, and may be subject to disciplinary action.

The OTSS shall develop and ensure compliance with policies and procedures necessary to monitor, manage and mitigate security and privacy risks.

8. The CIO shall provide regular updates – as well as an Annual State of Security, Privacy, and Data Governance Report – to the State Superintendent of Public Education that addresses the security and privacy posture and status of the MDE. These regular updates and annual report shall include at a minimum the status of the following:

    a. Audits and Mitigation
    b. Incidents
    c. Training
    d. Upgrades and Enhancements

9. All public schools – and charter schools, if required by the authorizer or in the charter contract – shall create LEA-wide policies, standards, and procedures outlined in Section 6 above. The policies will ensure that LEAs implement and maintain the appropriate security measures to protect and safeguard the agency, its users, and data from forms of unauthorized access, malicious misuse, disclosure, modification, or inadvertent compromise. The requirements and standards shall adhere to ITS' Enterprise Security Policy and shall not be less than those established by the MDE and OTSS. The more restrictive policy shall take precedence in the event of a conflict between the LEA's policy and MDE's policy.

    LEAs shall notify the MDE ISO in writing of any incident of cyber-attack, data breach, or violation of state/federal security and privacy laws and regulations within twenty-four (24) hours of the LEA becoming aware of the incident, breach or violation.

    LEAs shall cooperate with the MDE and its appointee(s) regarding any investigations into an incident of cyber-attack, data breach, or violation of this rule or state/federal security and privacy laws and regulations. The LEA shall share any root cause, postmortem, or final report that they generate regarding an incident of cyber-attack, data breach, or violation of this rule, state/federal security and privacy laws and regulations with the MDE and its appointee(s).

Source: 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)