

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

**OFFICE OF TECHNOLOGY AND STRATEGIC SERVICES**

- C. 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

State Board Policy Chapter 55, Rule 55.1 will provide guidance to the MDE regarding its operational responsibilities as it relates to Data Governance, Security, and Privacy, and the role of the Office of Technology and Strategic Services (OTSS) in meeting those operational responsibilities. The proposed revision will further provide guidance to OTSS regarding its role in supporting Local Educational Agencies as they address their local Data Governance, Security, and Privacy responsibilities.

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, 42 USC 1758 (b)(2)(C)(iii), Richard B Russell National School Lunch Act (42 U.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)*

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

3  
4 The Office of Technology and Strategic Services (OTSS) is to support the strategic mission and  
5 vision of the State Board of Education (SBE). To accomplish the support of the strategic mission  
6 and vision, OTSS will implement and support sound governance, a secure and stable  
7 infrastructure, reliable systems and applications, and quality data controlled within the  
8 Mississippi Department of Education (MDE). The MDE is committed to compliance with federal  
9 and state laws regarding data security and privacy.

- 10  
11 1. The OTSS's broad, operational responsibilities, the SBE charges OTSS with:
- 12
  - 13 a. Validating and managing data, documenting and managing data definitions,  
14 establishing and supporting workflow processes, and implementing and managing  
15 business rules established by Program Offices, state, and federal law for all data  
16 that is submitted to or collected by the MDE;
  - 17 b. Managing all information technology resources, including physical, virtual, and  
18 cloud;
  - 19 c. Ensuring the availability and integrity of systems and applications managed by  
20 the MDE;
  - 21 d. Securing networks, systems, and data, including monitoring and mitigating  
22 against threats;
  - 23 e. Granting access to information technology systems, applications, data, and reports  
24 to appropriate users;
  - 25 f. Managing database and data flows, analyzing data, and generating reports;
  - 26 g. Adhering to information technology best practices, and state and/or federal  
27 mandates and guidelines regarding the collection, storage, and disclosure of  
28 personally identifiable information (PII) of students, educators, parents, and MDE  
29 personnel.
- 30
- 31 2. The OTSS's specific responsibilities related to security, privacy, and governance, the  
32 SBE charges OTSS with:
- 33
  - 34 a. Staffing OTSS leadership positions with specific security, privacy and governance  
35 responsibilities;
  - 36 b. Establishing and supporting an agency-wide data governance program;
  - 37 c. Developing and administering internal policies and procedures necessary to  
38 ensure security and privacy;
  - 39 d. Providing mandatory security, privacy and governance training to all MDE  
40 personnel
  - 41 e. Developing and ensuring compliance with policies and procedures necessary to  
42 monitor, manage and mitigate security and privacy risks;
  - 43 f. Regularly reporting on the security and privacy posture and status of the MDE to  
44 the State Superintendent of Public Education;
  - 45 g. Sharing with public school districts information technology best practices, and  
46 state and/or federal mandates and guidelines regarding the collection, storage, and

47 disclosure of personally identifiable information (PII) of students, educators,  
48 parents, and MDE personnel.  
49

50 3. The following terms shall have the meanings ascribed to them in this section unless the  
51 context otherwise requires:

- 52 a. “Authorized User” is a consumer of information technology and data that has  
53 been entrusted access based on the principal of least privilege to perform a  
54 function for the MDE.
- 55 b. “Building consensus” is the mediation of a conflict involving many parties.
- 56 c. “Business Analyst” is a person who performs analysis of an information system’s  
57 requirements, functions, and interdependencies used to characterize system  
58 contingency requirements and priorities in the event of significant disruption.
- 59 d. “Change Management” is the process of regulating and approving changes to  
60 hardware, firmware, software, and documentation throughout the development  
61 and operational life cycle of an information system.
- 62 e. “Data” is the raw un-synthesized facts and statistics collected for reference or  
63 analysis.
- 64 f. “Data Steward” is the program office designee who is responsible for determining  
65 how data are defined, collected, audited, and reported to meet the program office  
66 and agency requirements.
- 67 g. “Escalating issues” is the act of bringing an item that has stalled in the resolution  
68 process to the attention of the person(s) who have the ability to direct a resolution  
69 path.
- 70 h. “Executive Leadership Team (ELT)” is the leadership team composed of the State  
71 Superintendent of Public Education and his/her division chiefs and designated  
72 leaders.
- 73 i. “Governance” is the agency-wide structure and processes for collaborative  
74 decision-making and management of the MDE data assets to improve quality and  
75 use, while enhancing security and privacy protections.
- 76 j. “Incident” is an occurrence that potentially jeopardizes the confidentiality,  
77 integrity, or availability of an information system or the information the system  
78 processes, stores, or transmits or that constitutes a violation or imminent threat of  
79 violation of security policies, security procedures, or acceptable use policies.
- 80 k. “Information” is the synthesized data that is a representation of knowledge useful  
81 for analysis.
- 82 l. “Information Technology” are systems for creating, consuming, transmitting, or  
83 storing information or data.
- 84 m. “Local Education Agency (LEA)” are districts within the state that are governed  
85 by the MDE.
- 86 n. “Mitigation” is the action of reducing the severity, seriousness, or damaging  
87 effects of risk or incident.
- 88 o. “The Principal of Least Privilege (POLP)” is providing access limited to the  
89 minimum rights and permissions an authorized user requires to perform their  
90 assigned function.
- 91 p. “Personally, Identifiable Information (PII)” is the information or data that could  
92 be combined to positively identify an individual (i.e. name, address, SSN)

- 93 q. “Risk” is a measure of the extent to which an entity is threatened by a potential  
94 circumstance or event.
- 95 r. “Systems” are a discrete set of information resources organized for the collection,  
96 processing, maintenance, use, sharing, dissemination, or disposition of  
97 information.
- 98 s. “Threat” is any circumstance or event with the potential to adversely impact the  
99 MDE.
- 100
- 101 4. The OTSS leadership positions with specific security, privacy, and governance  
102 responsibilities:
- 103
- 104 a. The MDE Chief Information Officer (CIO) will have leadership responsibility for  
105 – and shall be dedicated to – the daily management and long-range vision and  
106 strategies of OTSS. This employee shall be charged with the following  
107 responsibilities, including but not limited to:
- 108 i. Ensuring OTSS’ goals and strategies support and further the Goals of the  
109 SBE Strategic Plan;
- 110 ii. Providing strategic leadership to the MDE’s information technology and  
111 data endeavors;
- 112 iii. Ensuring that OTSS is appropriately staffed with dedicated and qualified  
113 professionals to achieve the Goals of the SBE Strategic Plan;
- 114 iv. Establishing and maintaining project management and change  
115 management over the information technology and data of the MDE ;
- 116 v. Establishing and supporting data governance within the MDE;
- 117 vi. Serving as the signatory for all the MDE’s purchases and contracts in  
118 relation to information technology, operational technology, and data;
- 119
- 120 b. The OTSS Information Security and Data Privacy Officer (ISO) shall be charged  
121 with the following responsibilities, including, but not limited to:
- 122 i. Ensuring the security, privacy, and governance of all data and information  
123 within the MDE, by establishing agency-wide policies for sustaining,  
124 enhancing, and protecting the privacy and confidentiality of the data;
- 125 ii. Working with the Data Governance Committee to improve and support  
126 data security and privacy through the Data Governance Policy;
- 127 iii. Investigating and reporting any complaints of privacy violations, data  
128 breaches and/or cyber-attacks under MDE’s jurisdiction – as well as  
129 coordinating with the appropriate authorities
- 130 iv. Identifying risks and threats to the MDE’s information systems and assist  
131 in remediation of these risks in coordination with OTSS;
- 132 v. Investigating and reporting issues of compliance – with this rule and with  
133 other applicable data security and privacy laws – by the MDE;
- 134 vi. Monitoring and reporting on data privacy, security, and governance  
135 training and compliance to the CIO and State Superintendent of Public  
136 Education;
- 137

- 138 c. The OTSS Data Governance Manager shall be charged with the following  
139 responsibilities, including, but not limited to:
- 140 i. Facilitating and coordinating the development, implementation, and  
141 maintenance of the MDE Data Governance Program to promote data  
142 quality, availability, usability, security, and privacy;
  - 143 ii. Supporting the Data Governance Committee chair, providing facilitation  
144 for and coordination among data governance members and workgroups;
  - 145 iii. Communicating with internal and external data governance stakeholders –  
146 including building consensus, mediating disputes, escalating issues,  
147 implementing resolutions, and anticipating agency data issues and needs;
  - 148 iv. Coordinating with data stewards and business analysts to document and  
149 analyze data processes and business rules – including engaging with  
150 various stakeholders to ensure awareness, buy-in, and compliance with  
151 data quality, security and privacy processes, and rules;
  - 152 v. Coordinating the development and adoption of key data governance  
153 artifacts - including data governance charter, guidelines, and a data  
154 dictionary;
  - 155 vi. Coordinating the development and adoption of key data policies (*See*  
156 *Section 6*);
  - 157 vii. Coordinating with the OTSS project managers to ensure that the  
158 prioritized agenda and project plans for key data governance artifacts and  
159 data policies are included in an agency-wide project portfolio.
- 160
- 161 5. The OTSS shall establish and support the agency-wide Data Governance program. This  
162 program shall be charged with the following responsibilities:
- 163
- 164 a. The MDE Data Governance program shall be implemented through the Data  
165 Governance Committee (DGC) comprised of members representing program  
166 offices across the MDE. The work of the DGC shall be authorized through the  
167 Data Governance Charter, as approved by the State Superintendent of Public  
168 Education. The DGC shall develop and promulgate processes, as well as rules  
169 and regulations governing the data that shall apply to all program offices within  
170 the MDE.
  - 171
  - 172 b. The DGC shall establish policies and processes to ensure that data collected by  
173 the MDE are stored, maintained, and disseminated in a manner that protects the  
174 data integrity and security, as well as the privacy of individuals involved. This  
175 includes specifying which data may or may not be collected by the MDE, as well  
176 as oversight and responsibility for ensuring the accuracy and validity of the Data  
177 Dictionary.
  - 178 i. The MDE program offices shall provide proposed changes to data  
179 collection no later than 30 days after SINE DIE. Change requests  
180 submitted after the 30-day mark will be held over for the future change  
181 request season unless otherwise approved by the State Superintendent of  
182 Public Education or his/her designee.

- 183                   ii. The DGC shall review and vote on all proposed changes by or before the  
184                   September committee meeting.
- 185                   iii. The DGC shall publish the Data Dictionary by December 1<sup>st</sup> in  
186                   preparation for the upcoming school year.
- 187                   iv. The DGC shall establish policies and processes to ensure that these annual  
188                   deadlines are met.
- 189
- 190                   c. The DGC shall prioritize and approve a set of internal policies, procedures,  
191                   standards, and guidelines – as well as a schedule for their development and  
192                   implementation – necessary to meet the security and privacy obligations of the  
193                   MDE.
- 194
- 195                   6. OTSS shall develop and maintain internal policies, procedures, standards, and guidelines  
196                   – approved by the DGC in accordance with the agency’s data governance process – that  
197                   are consistent with pertinent industry standards.
- 198
- 199                   a. Pertinent industry standards include
- 200                   i. The National Institute of Standards and Technology’s (NIST) current  
201                   Privacy Framework.
- 202                   ii. NIST’s current Cybersecurity Framework
- 203                   iii. NIST’s current SP 800-171 Protecting Controlled Unclassified  
204                   Information in Nonfederal Systems and Organizations
- 205                   iv. NIST’s current FIPS- 200 Minimum Security Requirements for Federal  
206                   Information and Information Systems
- 207                   v. FedRAMP’s current standards
- 208
- 209                   b. OTSS shall review on at least a biennial basis its internal policies, procedures,  
210                   standards, and guidelines to ensure consistent alignment with current industry  
211                   standards.
- 212
- 213                   c. To support LEAs, OTSS shall make available guidance, best practices, and  
214                   pertinent industry standards on the Information Security and Data Privacy section  
215                   of the MDE’s website
- 216
- 217                   d. OTSS shall encourage LEAs to develop and implement internal policies,  
218                   procedures, standards, and guidelines consistent with pertinent industry standards.
- 219
- 220                   7. In the event that an LEA becomes aware of a cybersecurity risk or threat that may  
221                   potentially impact the MDE, the State Network Consortium, or other LEAs, the impacted  
222                   LEA shall notify the MDE ISO within 24 hours to ensure that the MDE is able to  
223                   properly mitigate and coordinate a response to the emerging risk or threat, including  
224                   notifying other LEAs.
- 225
- 226                   8. The OTSS shall develop and support MDE staff compliance with all policies and  
227                   procedures necessary to monitor, manage, and mitigate security and privacy risks.
- 228



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

232  
233 MDE employee access to the MDE information technology and data shall be dependent  
234 upon their compliance with training completion and adherence to security and privacy  
235 policies, procedures, standards, and guidelines. Those who fail to complete this training  
236 or to adhere to the security and awareness program may be referred to ELT for  
237 termination of systems and network access and may be subject to disciplinary action.

238  
239 The OTSS shall develop and ensure compliance with policies and procedures necessary  
240 to monitor, manage and mitigate security and privacy risks.

241  
242 9. The CIO shall provide a quarterly report to the State Superintendent of Public Education  
243 regarding the security and privacy posture and status of the MDE. This quarterly report  
244 shall include at a minimum the following status on:

- 245
- 246 a. Audits and Mitigation
- 247 b. Incidents
- 248 c. Training
- 249 d. Upgrades and Enhancements

250  
251  
252 Source: Miss. Code Ann. §§ 25-53-1 through 25-53-25, § 25-53-201, § 25-61-1 *et seq.*, § 37-1-3,  
253 § 37-3-5, § 37-151-9, § 75-24-29 *et seq.*, MS ITS Enterprise Security Policy Miss. Admin. Code  
254 36: 1 *et seq.*, Every Student Succeeds Act (ESSA), Individuals with Disabilities Education Act  
255 (IDEA), Family Educational Rights and Privacy Act (FERPA), Richard B. Russell National  
256 School Lunch Act (NSLA), Children’s Online Privacy Protection Act (COPPA), Protection of  
257 Pupil Rights Amendment (PPRA), Children’s Internet Protection Act (CIPA), Federal  
258 Information Security Management Act of 2002 (FISMA), National Institute of Standards  
259 Technology (NIST), Federal Information Processing Standards 200 (FIPS)