OFFICE OF EDUCATIONAL ACCOUNTABILITY
Summary of State Board of Education Agenda Items
May 17-18, 2012

OFFICE OF MANAGEMENT INFORMATION SYSTEMS

42. Approval of the adoption of an agency-wide Information Technology Security Policy

Recommendation: Approval

Back-up material attached

Mississippi Department of Education

Office of Management Information Systems
IT Security Policy

Executive Summary

April 12, 2012

I. Introduction

As part of the Mississippi State Board of Education, the Mississippi Department of Education (MDE) is required to maintain confidentiality, integrity, and availability of the data stored and supported on their technology network infrastructure. In so doing, the Office of Management Information Systems (MIS) has created this IT Security Policy (Policy).

This policy was developed in accordance with the Federal Information Security Management Act of 2002 (FISMA) - the National Institute of Standards and Technology (NIST), the Federal Information Processing Standards 200 (FIPS), the Family Educational Rights and Privacy Act (FERPA) and the Mississippi Department of Information Technology Services – Enterprise Security Policy.

II. IT Security Policy Scope

This IT Security Policy applies to MDE agency-wide to include the Mississippi School for the Blind, the Mississippi School for the Deaf and the Mississippi School of the Arts.

III. MDE's Statutory Authority

MDE has developed this Security Policy under the following provisions and has followed the format and guidelines of NIST FIPS 200 Standards - Security Requirements for Federal Information and Information Systems, the Mississippi Department of Information Technology Services – Enterprise Security Policy and the Family Educational Rights and Privacy Act (FERPA).

The Family Educational Rights and Privacy Act (FERPA):

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Mississippi Department of Information Technology Services (ITS):

The provisions of § 25-53-1 to § 25-53-25 of the Mississippi Code Annotated detail the powers and duties of the Mississippi Department of Information Technology Services (ITS), including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

The Federal Information Security Management Act of 2002 (FISMA):

The Federal Information Security Management Act of 2002 (FISMA) - the National Institute of Standards and Technology (NIST), and the Federal Information Processing Standards 200 (FIPS).

Other Statutory and Legal Considerations:

Other statutory and legal requirements considered in preparation of this Security Policy include:

The No Child Left Behind Act of 2001 disaggregation requirements.

The Individuals with Disabilities Education Improvement Act of 2004 (IDEA) 34 CFR 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) and Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq.) or the Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.).

The Mississippi Public Records Act of 1983, Section 25-61-1, et seq. and state statutes on the confidentiality of education records, Section 37-15-3, 37-15-6 and 37-23-137 of the Mississippi Code of 1972, as amended, protecting the confidentiality of permanent records, cumulative folders, disciplinary records and records of special education students.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers.

IV. IT Security Administrative Safeguards

Security responsibilities for protecting the network infrastructure and related data and information are defined as Administrative Safeguards. The three safeguards that comprise the IT Security Administrative Safeguards are Agency (MDE) Responsibility, User Responsibility and MIS Responsibility.

Agency (MDE) Responsibility:

The IT Executive Steering Committee (ITESC) within MDE serves as an oversight committee. It oversees the security related activities of MDE and is responsible for the review, approval and the evaluation process of the MDE IT Security Policy.

User Responsibility:

MDE system access is strictly limited to staff employed (user) by the Department and individuals under contract (user) with the Department that have been expressly authorized access pursuant to this policy. This policy also covers access by parents and eligible students as defined by FERPA (34 CFR Section 99.3).

MIS Responsibility:

The network is housed in a Data Center located within the MDE facility. MDE must make every effort to ensure the confidentiality, integrity and availability of the MDE network infrastructure to include computer assets, data and information.

V. Technology, Data and information Access and Ownership

Data and Information Access:

For purposes of this policy, data and information is defined as any and all MDE data and information whether electronic or in paper form to include all student data and information MDE stores and processes in MSIS. This includes student records and free and reduced-price eligibility information for Federal and State programs.

Ownership of Data and information:

All MDE data and information developed, accessed and used by users in the course of performing their assigned duties and responsibilities shall be the exclusive property of MDE.

Ownership of Computer Equipment:

All computer equipment including, but not limited to computers, monitors, laptop computers, printers/scanners/copiers, smart phones, PDA's and peripheral equipment that are assigned to users are the property of MDE.

VI. IT SECURITY POLICIES

The follow table outlines the NIST-FIPS high-level security requirements. This outline comprises a total of 171 individual security requirements:

Control identifier	Security Policy
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Certification, Accreditation, and Security Assessments
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity