

**INFORMATION SECURITY POLICY
AT
MISSISSIPPI STATE UNIVERSITY**

Operating Policy and Procedures

Purpose

The purpose of this Operating Policy is to create a campus environment that promotes and verifies the proper security of information at all levels of Mississippi State University (MSU).

Background. Information security incidents are receiving enormous attention with the increasing number of leaks of protected information and cases of identity theft. Moreover, the threat of natural disaster requires physical security of the institution's information assets and plans for timely resumption of business in the wake of such an event.

MSU is subject to numerous federal and state laws and regulations regarding the protection of data, among them:

1. The Family Educational Rights and Privacy Act of 1974, (FERPA) commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access of educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.
2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes significant privacy requirements by creating national standards to protect personal health information.
3. The Gramm-Leach-Bliley Act (GLBA), while targeted at financial institutions, requires universities to maintain an information security program for the protection of financial information.
4. The Payment Card Industry (PCI) Data Security Requirements apply to all members, merchants, and service providers that capture, store, process, or transmit credit card data.

Major universities are in a unique position with large amounts of educational, medical, financial, and other critical information. The risks associated with an information security breach or significant data loss demands a strong Information Security Policy.

Policy

It is the policy of Mississippi State University to protect critical information in all forms for which it is the custodian and to maintain a robust, proactive, and evolving information

security program. This includes protection from a variety of threats such as fraud, embezzlement, sabotage, terrorism, extortion, privacy violation, service interruption and natural disaster.

Information security is the responsibility of all individuals who access and maintain Mississippi State University information resources, i.e. students, employees, alumni, affiliates, contractors, and retirees, and others as appropriate. Each individual must be aware of, committed to, and accountable for their role in the overall protection of critical information.

Procedure

Security of protected information is a complex issue, requiring a multi-faceted framework. While technology provides numerous tools to facilitate safeguarding of protected information, ultimately institutional awareness, commitment, vigilance, and persistence are the keys to a successful program.

In addition to personal accountability, other elements of MSU's information security framework mandated by this policy include:

- The Information Security Program – The program identifies technologies, procedures, and best practices to ensure ongoing institutional focus on the protection of information. Key elements of the Information Security Program include:
 - Data Classifications and Individual Responsibilities
 - Risk Assessment
 - Safeguards
 - Training
 - Awareness
 - Monitoring
 - Audit and Compliance

- The Incident Response Plan – The plan prescribes procedures to effect a timely and appropriate response in the event of an information security breach. Key elements of the plan include:
 - Incident Reporting
 - Investigation
 - Communication
 - Forensic Analysis
 - Post-mortem

- The IT Disaster Recovery Plan – The plan mandates procedures to effect the timely and orderly restoration of information technology resources and services in the event of a significant interruption or natural disaster. Key elements of the plan include:
 - Organizational Preparedness

- Continuity of Critical Applications
- Restoration of Normal Operation
- The Committee for the Security of Protected Information - This body is charged with oversight and coordination of the Information Security Program, the Incident Response Plan, and the IT Disaster Recovery Plan. The committee will review significant security incidents and recommend appropriate action and remediation.

It is expected that the individual components within the overall policy framework will continually evolve in response to changing information security technologies, requirements, and threats.

Related Policies. The following are MSU policies which have relevance and application to information security:

- Access to Computing Resources OP 01.11
- Use of Computing and Network Resources OP 01.12
- World Wide Web Pages and other Electronic Publications OP 01.13
- Misuse of University Assets OP 01.19
- Social Security Number Usage OP 01.23
- Buckley Amendment AOP 10.06
- Electronic Communications Infrastructure AOP 30.04
- Records Management and Security HRM 60-109
- Credit/Debit Card Processing OP 62.08
- Student Use of Computing Resources OP 91.117

Review

This OP will be reviewed every four years (or whenever circumstances require immediate review) by the Chief of Staff of the President’s Office in consultation with the University Committee for the Security of Protected Information. Recommendations for revision will be presented to the President.

OP 01.10
02/07/07

Authorization

AUTHORIZED BY:

/s/ Michael J. McGrevey
Chief of Staff of the President’s Office

11-15-06
Date

REVIEWED BY:

/s/ Don Zant
Director, Internal Audit

11-15-06
Date

/s/ Charles Guest
General Counsel

11-20-06
Date

APPROVED:

/s/ Robert H. Foglesong
President

02-07-07
Date