Mississippi State University
Operating Policy and Procedure
Access to Systems Containing Sensitive Information

PURPOSE

To define the requirements associated with granting access to information systems containing sensitive information and to define the ramifications of the misuse of such information systems.

SCOPE

For purposes of this policy, SYSTEM is defined as any university information system, electronic or paper, that contains Category I or II data as defined in the Information Security Policy, OP 01.10, and associated Information Security Program. This policy applies to anyone who needs access to a SYSTEM, including but not limited to employees, student workers, graduate assistants and University affiliates.

POLICY

Requests for access to a SYSTEM will be in line with University procedures.

PROCEDURE

Requests for SYSTEM access must be initiated via established procedures. Access to Banner, for example, requires submission of a Banner Access Request Form. To access all SYSTEMs, the following procedures also apply:

Employees and Student Workers:

- If they have not already done so, student workers must complete a support staff application for employment
- Will be subject to the University's criminal background screen policy HRM 60-122
- Must complete MSU's Information Security Training program
- Will be subject to the University's Guidelines for Employee Conduct HRM 60-401.
- Misuse of the SYSTEM may result in revocation of access and disciplinary action, up to and including separation from employment. Employees and student workers separated from employment will be subject to HRM 60-405, Separation of Employment. In addition, student workers will be subject to disciplinary action under Student Affairs policies and procedures.

Graduate Assistants:

- Will be subject to the University's criminal background screen policy HRM 60-122
- Must complete MSU's Information Security Training program
- Misuse of the SYSTEM may result in revocation of access and disciplinary action which will be referred to the Office of Graduate Studies.

Affiliates:

- Must complete MSU's Information Security Training program
- Must adhere to all university policies and procedures regarding confidentiality and security of information.
- Misuse of the SYSTEM will be reported to the appropriate authority and may result in revocation of access.

Routine revocation of SYSTEM access for an individual is the responsibility of the employing or sponsoring department and must be initiated when such access is no longer required by the work assignment. For example, revocation of access to Banner is initiated via the Banner Access Request Form with the "Access Expiration Date" field specifying the date on which access should be terminated.

Other Related Policies. The following are MSU policies which have relevance and application:

- Information Security Policy OP 01.10
- Access to Information Technology Resources OP 01.11
- Use of Information Technology Resources OP 01.12
- Misuse of University Assets OP 01.19
- Social Security Number Usage OP 01.23
- Buckley Amendment AOP 10.06
- Records Management and Security HRM 60-109
- Credit/Debit Card Processing OP 62.08

REVIEW

This policy and procedure will be reviewed by Mississippi State University's Information Security Committee at least every four years.

RECOMMENDED BY:

Mike Rackley 5/23/2011

For the Information Security Committee Date

Jerome A. Gilbert 5/25/2011

Provost and Executive Vice President Date

REVIEWED BY:

Lesia Bryant 6/02/2011

Director of Internal Audit Date

Joan L. Lucas 6/06/2011

General Counsel Date

APPROVED BY:

Mark Keenum 6/24/2011

President Date