OP 01.26: 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 OP 01.10 Information Security, 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:

- Will be subject to HRM 60.122 Criminal Background Checks
- Must complete MSU's Information Security Training program
- Will be subject to the HRM 60.401 Guidelines for Employee Conduct
- 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 HRM 60.122 Criminal Background Checks
- 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 the Graduate School.

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.

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

- OP 01.10 Information Security
- OP 01.11 Access to Information Technology Resources
- OP 01.12 Use of Information Technology Resources
- OP 01.19 Misuse of University Assets
- OP 01.23 Social Security Number Usage
- AOP 30.02 Education Records
- HRM 60.109 Records Management and Security
- OP 62.08 Credit-Debit Card Processing

REVIEW

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

REVIEWED BY:

/s/ Steve Parrott — 11/27/2017
Interim Chief Information Officer — Date

/s/ Judy Bonner — 11/27/2017
Provost and Executive Vice President — Date

/s/ Timothy N. Chamblee — 12/01/2017
Assistant Vice President and Director — Date
Institutional Research and Effectiveness

/s/ Joan Lucas — 11/29/2017
General Counsel — Date

APPROVED:

/s/ Mark Keenum — 12/06/2017
President — Date