OP 01.25: PRIVACY OF ELECTRONIC INFORMATION

PURPOSE

This policy defines the balance between the University's responsibilities and users' expectations of privacy when using Information Technology (IT) resources owned or provided by Mississippi State University (MSU).

POLICY

It is the policy of the University not to routinely monitor or examine individual use of MSU IT resources. However, individuals should have no expectation of privacy when using these resources as provided by MSU.

GUIDELINES

The University maintains electronic records on students and employees in central student and employee databases such as BANNER. Access to and release of information contained in these systems is governed by institutional policies, practices, and procedures, as well as state and federal laws and regulations (e.g. FERPA and HIPPA) and are beyond the scope of this policy.

The normal operation and maintenance of the University's IT infrastructure require the backup of data and communications, the logging of activity, the monitoring of usage patterns, and other such activities that are necessary for the provision of service. While also a normal activity, routine hardware and software maintenance of personal computers should be done, when practicable, in consultation with the user, their unit head, or the department's designated technical contact.

The University may monitor the activity, accounts, and electronic information of individual users when allowed by the user or it reasonably appears necessary to do so to protect the integrity or security of the University or its IT infrastructure. Also, IT log data is routinely captured and processed by Information Technology Services as part of operational requirements to monitor performance and aid in the detection and resolution of IT problems. Unless required by law, allowed by other University policy (e.g. OP 04.01), or due to an emergency situation involving imminent threat to persons or property, release of log data (including electronic door access and network access) that can be associated with individual users or any other monitoring of, granting access to, or providing copies of the contents of individual user accounts, files, emails, or other electronic information requires written authorization from one of the following, in consultation with General Counsel:

- The Dean of Students, in the case of current or former students
- The Chief Human Resources Officer, in the case of current or former staff
- The Provost, in the case of current or former faculty

- The President or appropriate Vice President

Communications and electronic documents stored within the University's IT environment are also generally subject to the Mississippi Public Records Act to the same extent as they would be if made on paper.

REVIEW

This OP will be reviewed every four years, or sooner if needed, by the Chief Information Officer.

REVIEWED:

/s/ Steve Parrott — 8/24/2020
Chief Information Officer — Date

/s/ David R. Shaw — 8/24/2020
Provost and Executive Vice President — Date

/s/ Tracey N. Baham — 8/24/2020
Director — Date
Institutional Research & Effectiveness

/s/ Joan Lucas — 8/24/2020
General Counsel — Date

APPROVED:

/s/ Mark E. Keenum — 8/24/2020
President — Date