TITLE:	Privacy of Electronic Information
ORIGINATOR:	Chief Information Officer
APPROVAL DATE:	June 2, 2023
EFFECTIVE DATE:	June 2, 2023
PURPOSE:	To define the balance between the University's responsibilities and users' expectations of privacy when using technology resources owned and provided by MUW
SEE ALSO:	
REVIEWER:	Chief Information Officer
REVIEW DATE:	2026 and every 3 years thereafter

OPERATING DETAILS:

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

2. 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 are beyond the scope of this policy.

3. 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 or their unit head.

4. 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 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, or due to an emergency situation involving imminent threat to persons or property, release of individual data (including electronic door access and network access) must receive prior approval. This approval includes access to individual user accounts, files, emails, OneDrive, SharePoint, voicemail or other electronic information.

5. Individuals needing to access or information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must submit a written request to the University's President. Employees relinquish their rights to electronic resources upon termination or separation of employment.

6. 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.