UAM OPERATING PROCEDURE 250.6
RE: IT Information Security

June 1, 2017
Revised: September 17, 2020

Part I. Introduction: The University of Arkansas at Monticello (UAM) is committed to securing and protecting the confidentiality, integrity, and availability of institutional data as well as any Information Technology (IT) that store, process or transmit institutional data. With its rapid proliferation, information technology is increasingly the medium for institutional programs and services. Consequently, the increasing volume and sophistication of cyber security threats-including targeting phishing scams, data theft, and other online vulnerabilities-demand that we remain vigilant about securing our systems and information. Therefore, this policy establishes minimum standards and expectations regarding the security of information technology and serves to support and implement University of Arkansas Board Policy 285.1.

Part II. Policy Statement: The purpose of this policy is to provide a security framework that will ensure the protection of institutional data from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. Institutional data may be used for administration, research, teaching, or other purposes. The information security policy applies to all UAM faculty and staff, as well as to students acting on behalf of UAM, through service on University bodies such as task forces, councils and committees. This policy also applies to all other individuals and entities granted use of University institutional data, including, but not limited to, contractors, temporary employees, and volunteers.

Part III. Definitions: Authorization – the function of establishing an individual's privilege levels to access and/or handle information.
Availability – ensuring that institutional data is ready and suitable for use.
Confidentiality – ensure that institutional data is kept in strict privacy.
Integrity – ensuring the accuracy, completeness, and consistency of institutional data.
Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling institutional data without proper authorization and legitimate business.
Institutional information – information that UAM collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Part IV. Classification Levels: All institutional data is classified into one of three levels, based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.
When combining information, the classification level of the resulting institutional data must be re-evaluated independently of the source data's classification to manage risks.
The classifications levels are:

A. Restricted
Institutional data for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.
This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified. The data owner should make this determination as it is the data owner's responsibility to implement the necessary security requirements.

B. Confidential
Institutional data is classified as Confidential if it falls outside the Restricted classification, but it is not intended to be shared freely within or outside the University due to its sensitive nature and/or contractual or legal obligations.
Sharing of Confidential institutional data may be permissible if necessary to meet the University's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential institutional data to parties outside the University, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the institutional data: (ii) not to disclose the institutional data to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena; and (iii) to notify the University in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Confidential institutional data within the University must comply with the University or University of Arkansas systemwide policies.

C. Public
Institutional data is classified as Public if it is intended to be made available to anyone inside and outside of the University.

All institutional data should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No University-owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of the University's Disaster Recovery and Business Continuity Plan.

- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Part V. Access Control Policy:

- Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- Where possible and financially feasible, more than one person must have full rights to any university owned server storing or transmitting high risk data.
- Access to the network and servers and systems should be achieved by individual and unique logins, and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- As stated in the current campus policies on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to university-related documents or files is required specifically and solely for the proper operation of University units, and where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit manager and submitted to the Chief Information Officer ("CIO") for approval. All users must secure their username or account, password, and system access from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with policies established by UAM's Information Technology department.
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination unless access has been approved by the Chancellor's office.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
- Activities performed as administrator or superuser must be logged where it is feasible to do so.

- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

Part VI. Virus Prevention Policy:

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Part VII: Intrusion Detection Policy:

- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. When possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

Part VIII. System Security Policy:

- All systems connected to the university network must be current with security patches.
- All systems connected to the university network should have a vendor supported version of the operating system install unless there is an exception approved by the CIO.
- System integrity checks of host and server systems housing high risk institutional data should be performed.

Part IX. Information Technology Security Training Program: Information technology security training is required yearly for all faculty, staff, and student employees across the institution. This training will be conducted through the institution's Learning Management

System (LMS), Blackboard, providing a report to the Executive Council as to who has not completed the required annual training by unit during the training period.

Part X. Information Technology Security Committee: An Information Technology Security Committee is responsible for reviewing pertinent operating procedures and response plans, devising polices, development and implementation of a security program, and establishing security standards. The committee will meet quarterly to review the latest compliance audit reports for operating system patches, anti-virus issues, and intrusion detection trends, as well as to develop program goals and assess progress toward meeting those goals.

The committee will be made up of representatives from the following units across the institution:

- Information Technology - Chair
- Residence Life
- College of Technology – Crossett
- College of Technology – McGehee

A report will be created and provided to the Chancellor's office and Executive Committee after each quarterly committee meeting.

Part XI. Information Technology Security Support: Information Technology (IT) will be the main point of contact for security related issues and concerns. In the event of a security breach or the perceived security breach, IT should be contacted immediately. Based on IT's assessment, if there is a security breach, the Vice Chancellor for Finance and Administration will notify the Executive Council and the Office of General Counsel. The notification will include a description of the incident, the number of individuals impacted, the nature of the information affected, and actions taken to isolate and prevent further breaches. The Office of General Counsel shall, in turn, assist campus or unit officials with (i) determining the nature and extent of any notifications to affected persons that may be required by state or federal law and (ii) coordinating any investigations that may need to be conducted by law-enforcement organizations.

Information Technology can be contacted as follows:

CIO: Ms. Anissa Ross
Email: mailto:infotech@uamont.edu
Location: Harris Hall, 1st Floor
Telephone: (870) 460-1036