Data Security Policy

Policy #:	IT004.2
Policy Type:	University
Responsible Executive:	VP for Information Services
Responsible Office:	Information Technology
Originally Issued:	July 2008
Latest Revision:	April 5, 2023
Effective Date:	April 5, 2023

I. Policy Statement

ULM faculty, staff, and students who use ULM's technology resources must be sensitive to issues pertaining to system security and confidentiality of information.

II. Purpose of Policy

The policy and procedures detailed in this document were developed to ensure that users who have been granted access to University Information Technology (IT) Resources understand their responsibilities related to system security and confidentiality of information.

III. Applicability

This policy applies to university faculty, staff, students, contractors, and vendors who use, access, or otherwise employ the University's IT Resources.

IV. Definitions

DMZ, or demilitarized zone, refers to a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The DMZ adds an additional layer of security to an organization's local area network.

Encrypted refers to the process of encoding a message or other information so that only authorized parties can access it.

Firewall refers to a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules that establishes a barrier between a trusted network and an untrusted network, such as the Internet.

IT Resources refers to computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

Remote Desktop refers to a software or operating system feature that allows a personal computer's (PC) desktop environment to be run remotely off of one system (usually a PC, but the concept applies equally to a server or a Smartphone) while being displayed on a separate client device.

VPN, or virtual private network, refers to a system that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

V. Policy Procedure

System Security/Confidentiality of Information

Only properly authorized and approved persons may access network or computer facilities. Proper authorization is provided by the Office of Information Technology (OIT) staff in the form of an 'account', 'id', or 'sign on' issued in the name of the authorized person. Users are responsible for all activities that occur through an account that has been issued to them. By applying for and using an account on University computer systems, a person agrees to abide by the following statements. These statements are listed on the 'Application for Accounts' and are applicable to all computer resources at the University.

- I will use the ULM Office of Information Technology facilities for purposes associated with my official duties or studies at the University, only.
- I will not allow other persons to use my account.
- I understand that I have an obligation to protect University hardware, software, and data. I will not attempt to gain access to accounts, data, or systems for which I have no authorization.
- I understand that abuse of equipment or violation of security will result in loss of privilege to use the system and that serious offenses will result in more serious disciplinary action.
- I understand the ULM Office of Information Technology is co-owner of all files on the system and has all rights to those files.

Users may not permit other persons to access a network or host computer via their account. Any user who believes that the account has been compromised by another party must report this concern to the OIT Helpdesk at (318) 342-3333.

Due to the nature of an individual's work assignment and the information which is stored on ULM computer systems, employees (faculty, staff, and student workers) may have access to information which is private and confidential in nature, i.e., grades, financial information, payroll information, etc. It is the responsibility of people who have access to this type of data not to disclose this information except on a "need to know" basis.

Security of Paper and Electronic Documents (Sensitive Data)

Paper Documents

Materials, documents, etc. that the employee transports to and from the primary work site to the off-campus location are their responsibility and must be kept confidential and secure. The employee shall protect the University records from unauthorized disclosure or damage and shall comply with University policies and procedures regarding such matters. When being transported to a remote location, information must not be visible. When at the remote location, documents must be retained in a secure environment. Paper reports containing sensitive data should be protected and when no longer needed, they should be shredded.

Electronic Documents

Employees shall store student, financial, personnel, and business records and related information electronically:

a) on university-provided management systems such as Banner, Moodle, and ImageNow;
b) in secure, password-protected group server file shares available on university desktops via Remote Desktop. (Note: Microsoft OneDrive shares should not be utilized for this content.)

Student, financial, personnel, and business records and related information must NOT be stored on non-university computers or on other storage devices or mechanisms. However, faculty may utilize password-protected Moodle courses during the semester to maintain course-related grading records before they are transferred into Banner Gradebooks.

University faculty, staff, students, contractors, and vendors who use, access, or otherwise employ the University's IT Resources are required to use ULM OIT developed web forms. University faculty, staff, students, contractors, and vendors are prohibited from using third party web forms unless receiving an approved exception from OIT.

To request the development of a web form, go to https://webservices.ulm.edu/computersos to create a ticket under Web Development and attach the form in .doc/.pdf or type out the requested fields. Persons requesting web form development are to note the advance lead time necessary by OIT to produce the desired web form.

When working away from the campus network, employees must use only ULM's OpenVPN service to access confidential information stored in locations such as: (a) Banner INB, (b) ImageNow, (c) the group file-share server, and (d) individual office computers (via a Remote Desktop connection). Employees are granted the use of the ULM OpenVPN System, which allows access to campus resources from any internet/broadband connection. Employees who use the VPN must ensure their computer meets specifications, such as recent patches and virus control software, before accessing the VPN. Employees are not allowed to give others access to the VPN through their login. Employees may access the ULM OpenVPN System with the information in the following document: https://ulm.edu/it/documents/ulmvpnonwindows10.pdf.

Whenever feasible, employees should store confidential documents or other information essential to the mission of ULM on the centrally managed group file-share server, rather than a local hard drive or portable device. Employees are granted the use of drive shares that are to be used to store ULM work-related documents. These shares are considered to be protected storage that is fault-tolerant and backed up daily. Employees will have a share that will be accessible only to them, and also a group share that will be accessible from anyone in their group. Other shares can exist as needed. These shares are not to be used for storing personal information, such as family pictures, music, or any non-work-related items.

Responsibilities of Teleworking Supervisors

Supervisors who choose to consider teleworking for employees shall be responsible for:

- determining how the department will handle restricted access materials, security issues, and taking electronic or paper records from the primary workplace;
- ensuring that practices are consistent and compliant with state and University procedure and state and federal law in the use of technology.

Sensitive Data on Portable Media

Sensitive data is NOT to be stored on laptops, diskettes, CD, DVD, tapes, jump drives, or other portable media unless encrypted and password protected. Preferably this data should be kept only on group file shares.

ULM Firewall & Static IP Addresses

The ULM Campus is protected by a redundant firewall system that both protects the campus from the outside world and also protects servers that are on the DMZ network. Requests for firewall rule changes are to be made via the Helpdesk Ticketing System. Requests can be made for static IP addresses and will be reviewed by OIT for approval.

ULM Passwords and Login Practices

OIT will adhere to policy set forth by the State Office of Information Technology department for password management.

Adhering to the following guidelines should facilitate proper system security.

- Memorize your password(s). DO NOT write passwords down and post in easy to find locations. If you must write a password down, do so in a discreet manner and keep in a secure location.
- Do not share your password with anyone - not even someone from OIT. If someone needs access to your device (for example, to verify that it works), log on for them. If you ever receive a call from anyone asking for your password in order to verify something, require them to come to your office and verify the process in your presence.
- If an unfamiliar person wants to use your device, be certain to verify their identity and whether they have authority to use the system. If you are currently logged on to a system, log off before allowing them on.
- Do not leave your device unattended and logged on in an area available to unauthorized users. If you must leave for an extended period and there is a chance someone who should not access your device can do so, log off.
- If you suspect that someone knows your password, set a new one before your data can be compromised. If you need assistance, contact the Helpdesk at (318) 342-3333.
- If at any time the OIT is prompted that something is questionable with your University account/access, OIT does have the ability to immediately lock accounts as a precautionary measure to ensure a bad actor has not compromised your account and security access.

ULM 3rd Party Server Access

When an outside entity/company/vendor requires access to a ULM server resource, the ULM department with which they are working must request this access. Someone in the ULM department should contact the Helpdesk to open a ticket for this request. When approved, the access will be temporary and monitored by OIT staff. Any violations to this policy will cause their access to be denied.

Any Contractor who has access to ULM's information technology assets shall be required to complete cybersecurity training as per the University's Cybersecurity Awareness Training Policy.

VI. Enforcement

The Director of Information Technology is responsible for enforcement of the policy.

VII. Policy Management

A. Responsive Executive: Vice President for Information Services and Student Success

B. Responsible Officer for Policy Management: Director of Information Technology

VIII. Exclusions

N/A

IX. Effective Date

The effective date of this policy is the date it is adopted and signed by the President.

X. Adoption

This policy is hereby adopted on this 5th day of April 2023.

Recommended for Approval by:

Dr. Michael Camille
VP for Info Services and Student Success

Approved by:

Ron Berry

Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

N/A

XII. Revision History

Original adoption date: July 2008
Revised May 27, 2022. Replaces information on pages 53- 55 of the "Security of Data and Computing Resources" section of the 2008 "ULM Computing Center Policies and Procedures Manual."
Revised April 5, 2023. Revisions to the Electronic Documents section to discuss the mandated use of ULM OIT developed web forms. Revision to the ULM 3rd Party Server Access portion included information about required cybersecurity awareness training.