Cybersecurity Awareness Training Policy

Policy #:	IT001.3
Policy Type:	University
Responsible Executive:	VP for Information Services & Student Success
Responsible Office:	Information Technology
Originally Issued:	January 7, 2020
Latest Revision:	November 5, 2024
Effective Date:	November 5, 2024

I. Policy Statement

It is the policy of ULM to enhance the safety of its information technology assets from cyberattack by requiring all employees and contractors who have access to the university's Information Technology Assets to complete cybersecurity awareness training prior to gaining and/or continuing to access such assets.

II. Purpose of Policy

The purpose of this Policy is to: implement mandatory cybersecurity awareness training for all Employees and Contractors who have access to the university's Information Technology Assets as required by ACT 155 of the 2020 Regular Session of the Louisiana Legislature, HB 633, codified at LA R.S. 42:1267.

III. Applicability

This Policy applies to:

(1) All categories of University Employees are included whether employed full-time or part-time: Classified, Unclassified, Faculty, Adjunct, Casual Wage, Fellows, Graduate Assistants, Teaching Assistants, and Student Workers with access to university's Information Technology Assets

(2) Any Contractor who has access to the university's Information Technology Assets during the term of any contract and during any renewal period.

IV. Definitions

Contractor, means any independent individual (non-employee of ULM) having a contract with the university to provide Personal Services (professional, personal, consulting, or social services) wherein the scope of any such personal services includes the Contractor having access to the university's Information Technology Assets.

Cybersecurity Awareness Training Course, means a cybersecurity course (on-line or in-person) that is adopted and used by ULM for employee and Contractor training and that, at minimum, meets the requirements of Act 155 of the 2020 Louisiana Legislature including designed to focus on forming information security habits and procedures that protect information resources and teach best practices for detecting, assessing, reporting, and addressing information security threats.

Employee, means any member of the faculty, staff, administration (whether full-time, part-time, or casual wages), student workers, and graduate assistants with access to the university's Information Technology Assets.

Information Technology Assets, means any piece of software or hardware within an information technology environment; integral components of ULM's IT organization's systems and network infrastructure; any and all information technology equipment owned by ULM, including (but not limited to) personal computers, servers, and communication equipment; computer software, firmware, middleware, servers, systems, networks, workstations, data communications lines, and all other information technology equipment, used by and under the control of ULM; all technology, hardware, computers, servers, workstations, routers, switches, data communication lines, network and telecommunications equipment, Internet-related information technology infrastructure and other information technology equipment; and email systems.

Personal Services, means professional, personal, consulting, or social services as defined in the Louisiana Procurement Code and associated administrative codes (*see* Section XI).

V. Policy Procedure

A. Cybersecurity Awareness Training

a) Employees

i) New Employees: All new employees shall complete the cybersecurity awareness course no later than within the first thirty days of initial service or employment with ULM.

ii) Continuing Employees. Any person currently employed by ULM as of January 7, 2020 must complete the cybersecurity awareness training annually by December 31 for Calendar Year 2020, and by April 15 for each CY thereafter. Student workers and graduate students are required to complete the training on their first day of work prior to engaging in any other activity. In all cases, the annual training shall be completed by December 31 of the then calendar year

iii) Noncompliance. Access to ULM's Information Technology Assets will be revoked for new and continuing employees if the course is not successfully completed by the respective deadlines. Failure to complete the training in a timely manner shall constitute grounds for disciplinary action including up to termination of employment.

b) Contractors:

i) Any Contractor who has access to ULM's information technology assets pursuant to a contract between such Contractor and ULM, shall be required to complete cybersecurity training during the term of the contract and during any renewal period. Access shall not be granted to any such Contractor prior to completion of the course.

ii) Completion of cybersecurity shall be included in the terms of a contract let by ULM to a Contractor who has assess to ULM's Information Technology Assets.

iii) Noncompliance. Access to ULM's Information Technology Assets will be revoked for Contractors if the course is not successfully completed by the respective deadlines. Failure to complete the training in a timely manner is considered a material breach of the contract term and constitute grounds for contract termination for cause for repeated failure to comply with this Policy.

B. Cybersecurity Awareness Training Course

The course, at minimum, shall meet the requirements set forth in ACT 155, including content on informing security habits and best practices for detecting, assessing, reporting, and addressing information security threats. The course made available to state agencies by State Civil Service may be adopted for use at ULM.

C. Reporting

The ULM President or designee will periodically verify that Cybersecurity Awareness training has been done and report Employee and Contractor course completions to the State Civil Service Director by March 31 of each year for the previous year. The initial reporting date is March 31, 2022, for completions in the last quarter of 2020 and CY 2021.

D. Procedure

i) New Employees

a) The Director of Human Resources (or designee) will notify each new employee of the training requirement during the onboarding process and/or new employee orientation.

b) The Director of Information Technology (or designee) shall require proof of course completion prior to providing a new employee with access to the university's Information Technology System.

ii) Continuing Employees.

a) The Director of Human Resources will:

- notify all employees of this Policy and the mandatory training requirement;
- submit a completion report to the ULM President by March 15 for submission to the State Civil Service Director; and
- notify the Director of Information Technology and immediate supervisor of the non-completers.

iii) Contractors

a) The Director of Purchasing will:

- publish notice of the training requirement for Contractors on the Purchasing Department's web page and other related documents (i.e., RFPs, ITBs, etc.);
- include a new training requirement clause in all initial and renewal contracts with Contractors who have access to ULM's Information Technology Assets;
- submit a completion report to the ULM President by March 15 for submission to the State Civil Service Director; and
- notify the Director of Information Technology and the contract monitor for the respective contract of the non-completers.

E. Other Required Cybersecurity Training

OIT regularly conducts phishing campaigns to test if employees are vulnerable to phishing operations. Phishing is the practice of sending fraudulent communications in an attempt to steal sensitive information. These communications appear to come from a legitimate and reputable source, usually through email and text messaging.

Any employee who falls victim to the OIT phishing campaign or to a confirmed phishing attack from an outside bad actor is required to complete the "Phishing Awareness" course available in NeoED within 30 calendar days of notification. Access to ULM's Information Technology Assets will be revoked for the employee if the course is not successfully completed by the 30-day deadline. Access will not be restored until the training is complete. Failure to complete the training in a timely manner shall constitute grounds for disciplinary action including up to termination of employment.

VI. Enforcement

A. Employees. The immediate supervisor of the respective employee is expected to ensure that the subordinate employee completes the cybersecurity awareness training course in a timely manner consistent with this Policy.

B. Contractors. The contract monitor is expected to ensure that the Contractor completes the cybersecurity awareness training in a timely manner consistent with this Policy.

C. Access. The Director Information Technology is expected to ensure that access is not granted to any Employee or Contractor who has not completed the cybersecurity awareness training course in a timely manner consistent with the Policy.

VII. Policy Management

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

B. Responsible Officers for Policy Management

- Director of Human Resources – new employee onboarding and/or orientation and training management
- Director of Information Technology – course content
- Director of Purchasing – contract clauses and contractor compliance

VIII. Exclusions

NA

IX. Effective Date

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

X. Adoption

This amended policy is hereby adopted on this 5th day of November2024.

Recommended for Approval by:

Dr. Michael Camille, Vice President for Information Services & Student Success

Approved by:

Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

• ACT 155 of the 2020 Regular Session of the Louisiana Legislature, H.B. 633, effective 6/9/2020 (http://www.legis.la.gov/legis/BillInfo.aspx?s=20RS&b=ACT155&sbi=y), codified at R.S. 42:1267 (http://www.legis.la.gov/Legis/Law.aspx?d=1187594)
• State Civil Service General Circular Number 2020-058, October 20, 2020, "Cybersecurity Awareness Training Course Now Available"
https://www.civilservice.louisiana.gov/files/general_circulars/2020/GC2020-058.pdf

Louisiana Procurement Code, LA R.S. 39:1556 (10), (37), (42), and (54).
http://www.legis.la.gov/Legis/Law.aspx?d=96049

Louisiana Administrative Code, LAC 34:V.2503(A)1, 2, 3, and 5

XII. Revision History

Original adoption date: January 7, 2020

Revised March 20, 2021. Entire policy was rewritten.

Revised November 5, 2024. Revisions include requiring additional phishing training for certain employees and updating the policy to reflect Human Resources role in the training.