Computing Systems Security Breach Policy

Policy #:	IT007.1
Policy Type:	University
Responsible Executive:	VP for ISSS
Responsible Office:	OIT
Originally Issued:	October 29, 2014
Latest Revision:	June 6, 2023
Effective Date:	June 6, 2023

I. Policy Statement

The University of Louisiana Monroe's (ULM) Computing Systems Security Breach Policy defines the requirements and responsibilities for addressing security incidents to minimize the negative impact on the confidentiality, integrity, and availability of University information resources.

II. Purpose of Policy

The purpose of the Computing Systems Security Breach Policy is to detail the specific procedures that are to be utilized in the event of a Computing Systems Security Breach, including the required notice to affected individuals and other parties. Prompt detection and appropriate handling of these security incidents are necessary to protect information assets critical to the University's mission, preserve personal data privacy and confidentiality, and facilitate compliance with applicable laws and regulations.

III. Applicability

This policy applies to all persons affiliated with the University in any capacity, including staff, students, faculty, contractors, and alumni.

IV. Definitions

Computing Systems Security Breach – An actual or suspected event that may adversely impact the confidentiality, integrity, or availability of an IT resource used by ULM or any information processed, stored, or transmitted by those resources. IT resources include individual computers, servers, storage devices, and media, and mobile devices, as well as the information stored on them. A Computing Systems Security Breach may be caused by: (a) a virus/spyware infection (i.e., sent data/files to external address, malware, encrypting/destroying files); (b) an unsuspecting user who provides private information to a bad actor in response to a phishing or SPAM email; (c) an individual accessing information from a stolen ULM computer; or (d) a 3rd party with access to any of ULM's systems.

Highly Sensitive Information – Examples of highly sensitive information include but are not limited to:

1. Name, address, with date of birth.
2. Records protected by FERPA (Family Educational Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act of 1996), GLBA (Gramm-Leach-Bliley Act), or other applicable federal laws and regulations.
3. Research data or results prior to publication or filing of a patent application.
4. Information subject to contractual confidentiality provisions.
5. Security codes, combinations, or passwords.

Personal Information – The first name or first initial and last name of an individual in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

1. Social security number.
2. Driver's license number or state identification card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
4. Passport number.
5. Biometric data, which is defined as data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

V. Policy Procedure

In the event of a known or suspected security breach to any University based computer system, the Office of Information Technology (OIT) must be immediately contacted with the details of the matter. Reporting such an incident is a requirement of all persons affiliated with the University in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

To report an information security incident, individuals should contact one of the following offices:

- During regular business hours: ULM’s IT Helpdesk office at 318-342-3333
- Outside of normal business hours: University Police Department at 318-342-5350

Incident Response Protocol

1) Upon receiving a report of a Computing Systems Security Breach incident, the ULM official at the IT Helpdesk or the University Police Department will log all essential information.

2) The ULM official at the IT Helpdesk or the University Police Department will immediately contact the incident response manager (or designee) by phone and/or email. The incident response manager (or designee) will lead the incident response team.

3) Upon notification of a suspected or known information security breach, OIT will employ the Information Security Incident Response Plan and activate the Incident Response Team to engage with members of the university community as well as with appropriate outside agencies, such as law enforcement.

4) The incident response manager (or designee) will call the designated numbers on the IT emergency contact list. If appropriate, the incident response manager will also contact individuals in an affected department.

5) The incident response manager (or designee) will make an initial assessment of the reported information security breach.

6) Contacted members of the incident response team will meet or discuss the situation over the telephone/ZOOM to determine a response strategy.

7) The incident response team will create an incident ticket. Team members will document the incident and actions taken in response.

Team members will: (a) make copies of logs, email, and other communication for evidence preservation; (b) keep lists of witnesses; and (c) keep evidence as long as necessary to complete prosecution and beyond in case of an appeal. This content will be included on the incident ticket.

8) Team members will act according to the specific threat identified.

9) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

10) Team members will restore the affected system(s) to the “Pre-Breach” state.

11) The incident response manager (or designee) will: (a) notify the police and other appropriate external agencies, such as the LA State Police Cyber Unit (lafusion@la.gov), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Louisiana Attorney General of the incident; and (b) work with these agencies if prosecution of the intruder is possible.

12) If Personal Information or Highly Sensitive Information was, or is reasonably believed to have been, acquired by an unauthorized person as a result of a Computing Systems Security Breach, the Incident Response Team will consult with the President, Vice Presidents, Office of Marketing & Communication (OMC), and General Counsel to discuss ULM's public notification responsibilities, per Louisiana Revised statute LARS 51: 3074 : http://www.legis.la.gov/Legis/Law.aspx?d=322030.

ULM will immediately notify the Office of Federal Student Aid (FSA) at CPSSAIG@ed.gov in the event of an unauthorized disclosure or an actual or suspected breach of federal student aid applicant information or other sensitive personal information, as required by the Student Aid Internet Gateway (SAIG) Enrollment Agreement.

13) Team members will assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

14) The incident response manager (or designee) will oversee an after-action review which will focus on (a) reviewing all aspects of the incident response, (b) updating policies where necessary, and (c) recommending changes to prevent a similar occurrence from happening again. Upon management approval, the changes will be implemented.

VI. Enforcement

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

VII. Policy Management

Responsible Executive: Vice President for Information Services & Student Success
Responsible Officer for Policy Management: Director of the Office of Information Technology

VIII. Exclusions

N/A

IX. Effective Date

This policy goes into effect upon the date signed by the University President.

X. Adoption

This policy is hereby adopted on this 6th day of June 6, 2023.

Recommended for Approval by:

Dr. Michael Camille
VP for Information Services & Student Success

Approved by:

Ron Berry
Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

Louisiana Revised statute LARS 51:3074: http://www.legis.la.gov/legis/Law.aspx?d=322030

XII. Revision History

Original Adoption Date: October 29, 2014

Revised June 6, 2023. Revisions include placing the policy in the required policy template and major revisions to all parts of the policy.