LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION:	Information Technology	Number:	10.01.07
AREA:	Information Security		

SUBJECT: Information Security Incident Management Policy

I. PURPOSE

Incident management is a foundational element of an information security program that facilitates planning, detection, analysis, prioritization, and management of a cybersecurity incident that may occur within Lamar University. The policy is designed to support risk mitigation activities that stem from a computer-based security incident.

II. SCOPE

This policy applies to all Information Technology (IT) resources owned, contracted, and operated by Lamar University. All Lamar University affiliates are responsible for adhering to this policy.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A. INCIDENT RESPONSE

1. *Incident Response Planning*

1.1. The office of the Information Security Officer (ISO) must develop, recommend, and maintain an incident response framework that includes this policy and procedures to provide Lamar University with the ability to appropriately investigate a security incident. The framework must:

1.1.1. Identify roles, responsibilities, and oversight.

1.1.2. Identify and address capability gaps in incident management.

1.1.3. Include procedures ensuring that incident response documentation is disseminated to appropriate personnel, including but not limited to owners, custodians, IRM, and ISO.

1.1.4. Specify requirements for continuous improvement of incident response capabilities.

2. *Incident Response Training [IR-2]*

2.1. The Office of the ISO must facilitate training for:

2.1.1. Employees in the Office of the ISO, within one year of assuming incident response role, to serve as incident handlers to handle incidents.

2.1.2. Employees to recognize and report an incident in the information system, at least annually.

2.1.3. Custodians on procedures associated with incident response to work with incident handlers, as required by information system changes.

2.1.4. Information system users consistent with their affiliation.

3. *Incident Response Testing [IR-3]*

3.1. Incident response procedures and capabilities must be tested biennially to determine the overall effectiveness of identifying potential weaknesses or deficiencies. Capabilities in this context include but not limited to tools, technologies, training, and skills.

4. *Incident Handling Prioritization and Authority [IR-4]*

4.1. Incident response activities must include assessment of the significance of information security incidents based on the business impact of the affected resources and the current and potential technical effect of the incident.

4.2. The Incident response procedures and activities must prioritize containment, eradication, and recovery over root cause analysis.

4.3. An incident handler must be assigned to coordinate activities for each reported incident.

4.4. The incident handler is authorized to categorize a newly reported incident.

4.5. The incident handler may change the category of an incident, with the approval of the ISO, as more information is obtained during the investigation.

4.6. The incident handler, with the approval of the ISO, may collaborate with other Lamar University affiliates during the investigation and coordinate incident handling activities with contingency planning activities.

4.7. Lamar University affiliates must participate in incident investigations while maintaining confidentiality and secrecy.

4.8. The incident response documentation must be reviewed and updated, as needed, as part of continuous improvement of incident handling capabilities.

4.9. Under the direction of the ISO or the Lamar University Police Department (LUPD) and, the Office of the ISO is authorized to escalate or reduce privileges to any account to aid an incident investigation.

4.10. The Office of the ISO must incorporate lessons learned from ongoing incident handling activities and implement the resulting changes accordingly into the incident response procedures, training, and testing.

5. Incident Monitoring [IR-5]

5.1. The incident handler must maintain specific documentation based on the type of each incident to support forensics and trend analysis.

6. Incident Reporting [IR-6]

6.1. Lamar University affiliates must report an identified incident to the Office of the ISO.

6.2. Lamar University affiliates may not disclose incident particulars, directly or indirectly, including through social media, without written authorization from the office of the President.

6.3. In cases of incidents, the University must:

6.3.1. Report to Department of Information Resources (DIR) where the security incident is assessed to:

6.3.1.1. Propagate to other state systems.

6.3.1.2. Result in criminal violations that shall be reported to law enforcement in accordance with state or federal information security or privacy laws.

6.3.1.3. Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in Business and Commerce Code, §521.002(a)(2) and other applicable laws that may require public notification.

6.3.2. Contact law enforcement, as required, if the security incident is determined to have involved suspected criminal activity (e.g., violations of Chapters 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code (Telecommunications Crimes)).

6.4. In cases of “breach of system security” as defined by section 521.053 of the Business & Commerce Code of “Sensitive personal information”, the University must:

6.4.1. Comply with the notification requirements of Section 521.053 of the Business & Commerce Code.

6.4.2. No later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:

6.4.2.1. DIR, including the state’s chief information security officer.

6.4.2.2. If the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state.

6.4.3. No later than the 10th business day after the date of the eradication, closure, and recovery from a breach, suspected breach, or unauthorized exposure notify DIR, including the chief information security officer, of the details of the event and include in the notification an analysis of the cause of the event.

6.4.4. Notify Texas State University System, System Administration, via the Vice Chancellor and Chief Financial Officer and the Chief Audit Executive in accordance with TSUS Rules and Regulations, within similar timelines to reporting requirements specified in TAC 202.73b and TGC 2054.1125.

6.5. The Office of the ISO must submit monthly incident reports to DIR, in accordance with Chapter 202 of the Texas Administrative Code, TAC 202 §202.73.2.

6.6. All information relating to a security incident must be preserved at least 5 years unless stipulated by litigation requirements.

7. Incident Response Assistance [IR-7]

7.1. As an element of incident response capabilities, Lamar University must provide incident response resources that advise and assist users of information system in handling and reporting security incidents.

7.2. Incident response resources are determined by the ISO and may be comprised of technical support personnel, verified third-party consultants, and other resources.

7.3. Incident response activities may require highly specialized skills such as digital forensics and malware analysis, therefore, management supports the Office of the ISO to maintain the means of obtaining access to such skilled incident response support, during an incident.

V. EXCEPTIONS

A. The ISO, with the approval of the Lamar University President, may issue documented exceptions to controls in this policy based on justifications communicated as part of the risk assessment process.

VI. ENFORCEMENT

A. Failure to adhere to the provisions of this policy statement may result in:
1. Loss of Lamar University Information Resources access privileges.
2. Disciplinary action up to and including termination for employees, contractors, or consultants.
3. Dismissal for interns and volunteers.
4. Suspension or expulsion in the case of a student.
5. Civil or criminal prosecution.

VII. RELATED DOCUMENTS

A. Definition Catalog.
B. Lamar University Information Security Program.
C. Lamar University Incident Response Framework.
D. Lamar University Incident Response procedures.
E. Texas Administrative Code, RULE §202.
F. Texas State University System Rules and Regulations.
G. Texas State University System Glossary.
H. Texas Government Code 2054.
I. Texas Penal Code 33 and 33a.
J. Texas Business and Commerce Code 521.

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: N/A

Next Review Date: 04/11/2024

IX. APPROVAL

Signed 04/12/2021.

President, Lamar University

Signed 04/12/2021.

IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
1.0	04/12/2021	New Policy