LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Physical and environmental protection
AREA: Information Technology Area Number: 10.01.03

SUBJECT: PHYSICAL AND ENVIRONMENTAL PROTECTION

I. PURPOSE

This document establishes the physical and environmental protection policy for mitigating the risks to information systems residing in an information processing facility that are owned, contracted or operated by Lamar University from physical and environmental threats.

II. SCOPE

The Lamar University physical and environmental protection policy applies to all information custodians required to protect information and information resources. Information custodians are responsible for ensuring physical security controls and procedures are implemented either directly or contractually at facilities where information resources are hosted.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A.PHYSICAL AND ENVIRONMENTAL PROTECTION

1. *Physical Access Authorizations [PE-2]*
   - *1.1.* Information custodians must:
     - *1.1.1.* Develop, approve, and maintain a list of individuals with authorized access to the information processing facility.
     - *1.1.2.* Document, issue authorization credentials and provision physical access to information processing facilities, when appropriate.
     - *1.1.3.* Facilitate a review by the information system owner or the head of the department to assess the appropriateness of authorizations granted to individuals for physical access to information processing facilities every two years.
     - *1.1.4.* Revoke and de-provision physical access to individuals who are no longer authorized.

2. *Physical Access Control [PE-3]*
   - *2.1.* Information custodians must:
     - *2.1.1.* Enforce physical access authorization for all entry and exit points to the facilities where the information system resides by:
       - *2.1.1.1.* Validating individual access authorizations before granting access to the facility.
       - *2.1.1.2.* Controlling entry and exit to the facilities using university approved physical access devices, guards, or both. Examples of physical access devices include keys, locks, combinations, and card readers. Currently, card readers are the approved methods of controlling access by the university.
     - *2.1.2.* Maintain physical access audit logs for all entry and exit points to information processing facilities where information systems reside.
     - *2.1.3.* Implement surveillance cameras and monitor the cameras to control access to areas within the facility officially designated as publicly accessible.
     - *2.1.4.* Escort and monitor visitor activity if not explicitly on the list of individuals with authorized access to the information processing facility.
     - *2.1.5.* Secure physical access devices.
     - *2.1.6.* Inventory physical access devices annually. For example, Physical access devices include keys, locks, combinations, biometric readers, and card readers.
     - *2.1.7.* Change combinations and keys when keys are lost, combinations are compromised, or when authorized individuals are transferred or terminated.
     - *2.1.8.* Investigate information systems for signs of compromise in the event of unauthorized access and engage law enforcement and the office of the ISO.

3. *Access Control for Transmission Medium [PE-4]*
   - *3.1.* Information custodians must restrict and control physical access to and prevent tampering with network aggregation points, wireless access points, and other devices used to provide network access in data processing facilities in the university network.

4. *Access Control for Output Devices [PE-5]*
   - *4.1.* Information custodians must restrict and control physical access at facilities to information output devices to prevent unauthorized individuals from obtaining the output if the output contains confidential or regulated information. Examples of information system output devices include monitors, printers, copiers, scanners, fax machines, and audio devices.

5. *Monitoring Physical Access [PE-6]*
   - *5.1.* Information custodians must:

5.1.1. Monitor physical access to information processing facilities to detect and respond to physical security incidents.

5.1.2. Review physical access logs every 90 days or upon the occurrence of suspicious events. Examples of suspicious events include access outside of normal working hours, repeated access to areas not normally accessed, access for unusual lengths of time, and out-of-sequence access.

5.1.3. Coordinate the results of reviews and investigations in the event of unauthorized access and engage law enforcement and the office of the ISO.

6. *Visitor Access Records [PE-8]*

6.1. Information custodians must:

6.1.1. Maintain visitor access records to information facilities for one year. Visitor records for non-publicly accessible areas must include the name, organization of the visitor, the form of identification presented, date of access, systems accessed, time of entry and departure, the purpose of visit, and acknowledgment by the visitor to terms associated with the access granted.

6.1.2. Review visitor access records every 90 days.

6.1.3. Report anomalies in visitor access records to the office of the ISO.

7. *Power Equipment and Cabling [PE-9]*

7.1. Information custodians must ensure that power equipment and cabling for information systems are protected from damage and destruction.

8. *Emergency Power [PE-11]*

8.1. Information custodians must ensure that information processing facilities are equipped with an Uninterruptible Power Supply (UPS), when financially and technically feasible, to facilitate an orderly shutdown of the information systems in the event of loss of primary power source.

9. *Emergency Lighting [PE-12]*

9.1. Information custodians must ensure that information processing facilities are equipped with automatic emergency lighting that activates in the event of a power outage or disruption and that the lighting identifies emergency exits and evacuation routes.

10. *Fire Protection [PE-13]*

10.1. Information custodians must ensure that information processing facilities are equipped with fire detection and suppression systems, an independent energy source, and automated alerting of key personnel in the event of fire.

11. *Environmental Controls [PE-14]*

11.1. Information custodians must:

11.1.1. Maintain temperature and humidity levels within the information processing facilities according to manufacturers-defined acceptable levels.

11.1.2. Monitor environmental control levels continuously and key personnel are alerted when levels exceed thresholds.

12. *Water Damage Protection [PE-15]*

12.1. Information custodians must:

12.1.1. Ensure that facilities are equipped with a master shutoff that is accessible, working properly, and known to key personnel.

12.1.2. Ensure that facilities are equipped with monitoring systems that detect water leaks and alert key personnel.

12.1.3. Designate and train personnel that are responsible for responding to water leaks.

13. *Delivery and Removal [PE-16]*

13.1. Information custodians must:

13.1.1. Authorize, and control information system-related items such as hardware, firmware, and software entering and exiting the information processing facility.

13.1.2. Maintain records of Information system components that store or process confidential or regulated information. Examples of components include Storage Drives, Memory, and Portable storage devices.

14. *Alternate Work Site [PE-17]*

14.1. Information custodians must:

14.1.1. Determine and document Lamar University defined alternative worksites allowed for use by employees.

14.1.2. Employ Lamar University controls at alternate worksites.

14.1.3. Assess the effectiveness of controls at alternate worksites

14.1.4. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

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. Texas Controls Standards Catalog
B. TAC 202
C. NIST Special Publication 800.53 Rev 4

.

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: 07/14/2025

Next Review Date: 07/14/2028

IX. APPROVAL

Jaime Taylor – 09/25/2025

_____

President, Lamar University

Patrick Stewart – 09/25/2025

_____

IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
2	07/21/2025	Scope - Deleted context of term “information system custodian” and “information custodian” from scope, in line with TAC202 definition. PE 1 - Removed. PE 2 – Retention Period removed. 1.1.2 - New Language PE 8 – Report Anomalies added. PE 10 - Emergency shutoff removed. PE 13 – New Language PE 16 – New Language. PE 17 – New Language.