LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Physical and environmental protection
AREA: Information Technology Number 10.01.03
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 assets from physical security and environmental threats.

II. SCOPE

The Lamar University physical and environmental protection policy applies to all Information system custodians required to protect information and information resources. Information system custodians are responsible for ensuring physical security controls and procedures are implemented either directly or contractually at facilities where information resources are hosted.
In the context of this policy, the term information system custodian is used in place of Texas state defined custodian for clarity and to avoid conflict.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A.PHYSICAL AND ENVIRONMENTAL PROTECTION

1. *Physical and Environmental Protection Policy and Procedures [PE-1]*
   - *1.1.* Information system custodians are responsible for developing, implementing, and disseminating procedures and associated physical and environmental controls to relevant personnel and contractors.

2. *Physical Access Authorizations [PE-2]*
   - *2.1.* Information system custodians must:
     - *2.1.1.* Develop and maintain a list of individuals with authorized access to the information processing facility.
     - *2.1.2.* Document the authorization and provisioning of physical access to information processing facilities.
     - *2.1.3.* Retain the documentation for two years.
     - *2.1.4.* Review appropriateness of authorizations granted to individuals to physical information processing facilities every two years.
     - *2.1.5.* Revoke and de-provision physical access to individuals who are no longer authorized.

3. *Physical Access Control [PE-3]*
   - *3.1.* Information system custodians must:
     - *3.1.1.* Enforce physical access authorization for all entry and exit points to the facilities where the information system resides by:
       - *3.1.1.1.* Validating individual access authorizations before granting access to the facility.
       - *3.1.1.2.* Controlling entry and exit to the facilities using physical access devices, guards, or both. Examples of physical access devices include keys, locks, combinations, and card readers.
     - *3.1.2.* Maintain physical access audit logs for all entry and exit points to facilities where information systems reside.
     - *3.1.3.* Implement surveillance cameras and monitor the cameras to control access to areas within the facility officially designated as publicly accessible.
     - *3.1.4.* Escort and monitor visitor activity.
     - *3.1.5.* Secure physical access devices.
     - *3.1.6.* Inventory physical access devices annually.
     - *3.1.7.* Change combinations and keys when keys are lost, or combinations are compromised or when authorized individuals are transferred or terminated.
     - *3.1.8.* Investigate information systems for signs of compromise in the event of unauthorized access and engage law enforcement and the office of the ISO.

4. *Access Control for Transmission Medium [PE-4]*

4.1. Information system custodians must restrict and control physical access to and prevent tampering of network aggregation points, wireless access points and other devices used to access the University network.

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

6. *Monitoring Physical Access [PE-6]*
   6.1. Information system custodians must:
      6.1.1. Monitor physical access to information processing facilities to detect and respond to physical security incidents.
      6.1.2. 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.
      6.1.3. Coordinate the results of reviews and investigations in the event of unauthorized access and engage law enforcement and the office of the ISO.

7. *Visitor Access Records [PE-8]*
   7.1. Information system custodians must:
      7.1.1. Maintain visitor access records to information facilities for one year. Visitor records for non-publicly accessible areas must include name, organization of the visitor, 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.
      7.1.2. Review visitor access records every 90 days.

8. *Power Equipment and Cabling [PE-9]*
   8.1. Information system custodians must ensure that power equipment and cabling for information systems are protected from damage and destruction.

9. *Emergency Shutoff [PE-10]*
   9.1. Information system custodian must:
      9.1.1. Ensure that authorized personnel can shutoff power to information systems or individual components in an emergency.
      9.1.2. Ensure emergency shutoff switches or devices are placed in clear and accessible areas to facilitate safe and easy access for authorized personnel.
      9.1.3. Protect emergency shutoff capabilities from unauthorized

activation.

10. *Emergency Power [PE-11]*
    - *10.1.* Information system custodians must ensure that information processing facilities are equipped with an Uninterruptible Power Supply (UPS) to facilitate an orderly shutdown of the information systems in the event of loss of primary power source.

11. *Emergency Lighting [PE-12]*
    - *11.1.* Information system 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.

12. *Fire Protection [PE-13]*
    - *12.1.* Information system custodians must ensure that information processing facilities are equipped with fire suppression and detection systems, and an independent energy source, and automated alerting of key personnel in the event of fire.

13. *Temperature and Humidity Controls [PE-14]*
    - *13.1.* Information system custodians must ensure that temperature and humidity levels are monitored and maintained within the facility at optimal levels for the equipment, and key personnel are alerted when levels exceed thresholds.

14. *Water Damage Protection [PE-15]*
    - 14.1. Information system custodians must:
      - *14.1.1.* Ensure that facilities are equipped with a master shutoff that is accessible, working properly, and known to key personnel.
      - *14.1.2.* Ensure that facilities are equipped with monitoring systems that detect water leaks and alert key personnel.
      - *14.1.3.* Designate and train personnel that are responsible for responding to water leaks.

15. *Delivery and Removal [PE-16]*
    - *15.1.* Information system custodians must:
      - *15.1.1.* Authorize, document, monitor, and control information system-related items such as hardware, firmware, and software entering and exiting the facility.
      - *15.1.2.* Authorize, document, monitor, and control equipment deliveries and removals from the facility and maintain records of those items.

16. *Alternate Work Site [PE-17]*
    - *16.1.* Information system custodians must ensure physical and environmental protection controls are enforced at alternate worksites

designated in the Continuity of Operations Plan (CooP).

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: 06,02, 2021

Next Review Date: 06,02, 2024

IX. APPROVAL

_____
President, Lamar University

_____
IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
1.2	06,02, 2021	Changed the term custodian to information system custodian to distinguish between custodian roles in facilities. PE 1 - Assign responsibilities to custodian and language updated to match NIST. PE 2 – Assign responsibilities to custodian and created sub-items for existing points. PE 3 – Assign responsibilities to custodians, restored language from Texas controls standards catalog.