1. OVERVIEW AND PURPOSE

This document establishes the physical and environmental protection policy for mitigating the risks to information assets from physical security and environmental threats.

2. SCOPE

The Lamar University physical and environmental protection policy applies to all information custodians who are 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 assets are hosted.

The term "facility" generally refers to locations such as data centers and network and telecommunication closets in which information or information resources are housed, except for those areas within the facility officially designated as publicly accessible.

3. DEFINITIONS

See definition catalog version 2 or newer.

4. POLICY

The information custodian must enforce each control in this policy unless otherwise designated.

4.1 PHYSICAL AND ENVIRONMENTAL(PE) PROTECTION POLICY AND PROCEDURES

4.1.1 Ensure that this policy and associated procedures are disseminated to relevant personnel and contractors.

4.2 PHYSICAL ACCESS AUTHORIZATIONS

4.2.1 Develop and maintain a list of individuals with authorized access to the facility. Document the authorization and provisioning of physical access to facilities. Retain
the documentation for two years.

4.2.2 Review appropriateness of authorizations granted to individuals to physical facilities every two years.

4.2.3 Revoke and de-provision physical access to individuals who are no longer authorized.

4.3 PHYSICAL ACCESS CONTROL

4.3.1 Enforce physical access controls for all physical access points to the facility.
4.3.2 Validate individual access authorizations before granting access to the facility.
4.3.3 Control entry to the facility using physical access devices or guards or both.
4.3.4 Control access to areas officially designated as publicly accessible in accordance with the organization’s risk assessment.
4.3.5 Secure combinations, keys, and other physical access devices.
4.3.6 Inventory physical access devices yearly.
4.3.7 Change combinations when compromised.
4.3.8 Change locks when keys are lost.
4.3.9 Change combinations and locks when physical access devices cannot be recovered from individual who no longer authorized to access to facilities.
4.3.10 Investigate information systems for signs of compromise in incidents of unauthorized access and engage law enforcement and the office of ISO.

4.4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

4.4.1 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.

4.5 ACCESS CONTROL FOR OUTPUT DEVICES

4.5.1 Restrict and control physical access at facilities to information output devices to prevent unauthorized individuals from obtaining the output.

4.6 MONITORING PHYSICAL ACCESS

4.6.1 Monitor physical access to the information asset to detect and respond to physical security incidents.
4.6.2 Review physical access logs every 90 days and provide the results to the office of ISO.
4.6.3 Report any physical security incidents to the office of ISO immediately.

4.7 WITHDRAWN BY NIST

4.8 VISITOR ACCESS RECORDS

4.8.1 Restrict and control physical access to the information asset by authenticating visitors before authorizing access to the facility.
4.8.2 Maintain visitor access records to the facility. Visitor records must include name and organization of the visitor, form of identification presented, date of access and systems accessed, time of entry and departure, purpose of visit, and acknowledgement by the visitor to terms associated with the access granted.

4.8.3 Review visitor access records every 90 days.

4.9 POWER EQUIPMENT AND CABLING

4.9.1 Ensure that power equipment and cabling for the information asset is protected from damage and destruction.

4.10 EMERGENCY SHUTOFF

4.10.1 Ensure that authorized personnel can shut off power in an emergency.

4.10.2 Ensure emergency shutoff switches or devices are placed in clear and accessible areas to facilitate safe and easy access for authorized personnel.

4.11 EMERGENCY POWER

4.11.1 Ensure that facilities are equipped with an uninterruptible power supply (UPS) to facilitate an orderly shutdown of the information asset in the event of loss of primary power source.

4.12 EMERGENCY LIGHTING

4.12.1 Ensure that 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.

4.13 FIRE PROTECTION

4.13.1 Ensure that 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.

4.14 TEMPERATURE AND HUMIDITY CONTROLS

4.14.1 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.

4.15 WATER DAMAGE PROTECTION

4.15.1 Ensure that facilities are equipped with monitoring systems that detect water leaks
and alert key personnel.
4.15.2 Designate and train personnel that are responsible for responding to water leaks.
4.15.3 Ensure that facilities are equipped with a master shutoff that is accessible, working properly, and known to key personnel.

4.16 DELIVERY AND REMOVAL

4.16.1 Authorize, document, monitor, and control information system related items such as hardware, firmware, and software entering and exiting the facility.
4.16.2 Authorize, document, monitor, and control equipment deliveries and removals from the facility and maintain records of those items.

4.17 ALTERNATE WORK SITE

4.17.1 Ensure physical and environment protection controls are enforced at alternate worksites designated in the Continuity of Operations Plan.

4.18 EXCEPTIONS

4.18.1 The Information Security Officer, with the approval of the President, may issue documented exceptions to controls in this policy based on justifications communicated as part of the risk assessment process.

5. ENFORCEMENT
Failure to adhere to the provisions of this policy statement may result in:
5.1 Loss of Lamar University Information Resources access privileges,
5.2 Disciplinary action up to and including termination for employees, contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student, or
5.3 civil or criminal prosecution.

6. RELATED DOCUMENTS

7. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: February 20, 2018

Next Review Date: February, 20, 2021
8. **APPROVAL**

Kenneth Evans  
*President, Lamar University*  
February 20, 2018  
Date of Approval

Priscilla Parsons  
*Chief Information Officer, Lamar University*  
February 20, 2018  
Date of Approval

9. **REVISION HISTORY**

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Approved Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2/20/2018</td>
<td>This policy is a revision of IT Physical Access/Environmental Security Policy.</td>
</tr>
</tbody>
</table>