Sam Houston State University
A Member of The Texas State University System
Information Technology (IT)

IT Physical Access & Environmental Policy: IT-25

PURPOSE:

This policy is intended to establish standards for securing IT data centers, network closets and protected IT facilities on Sam Houston State University (SHSU) premises. Effective implementation of this policy will minimize unauthorized access to these locations, provide more effective auditing of physical access controls, and ensure environmental threats to IT data centers are monitored and remediated in a timely manner.

SCOPE:

The IT Physical Access Policy applies to IT data centers containing enterprise systems and other information processing facilities such as network closets, on-site back up storage locations, the corresponding network infrastructure and access across campus, and any other SHSU information resource facilities that serve the SHSU user community.

POLICY STATEMENT:

1. SHSU information resource facilities are restricted to authorized IT personnel only with the following exceptions:

    a. Access to certain information resource facilities may be granted only to SHSU support personnel and contractors whose job responsibilities require access to that facility.
    b. Visitors, individuals who have not been explicitly granted access rights, must always be escorted in restricted areas of information resource facilities.

2. Individuals granted access rights to an information resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

3. All information technology resource facilities that allow visitor access will track access with a sign in/out log.

4. Restricted access rooms should be identified with discrete signage.

5. The process of granting card and/or key access to information resource facilities must include the approval of the person responsible for the facility.

6. Access cards and/or keys must not be shared or loaned to others.

7. Access cards and/or keys that are no longer required must be returned to the appropriate department. Keys or cards must not be reallocated to another individual bypassing the return process.

8. Lost or stolen access cards and/or keys must be reported immediately to the appropriate department.

9. A service charge may be assessed for access cards and/or keys that are lost, stolen, or not returned.

10. Card access records and visitors logs for information resource facilities must be kept for routine review based upon the criticality of the information resources being protected.

11. The person responsible for the information resource facility must promptly remove the card and/or key access rights of individuals that change roles within SHSU or are separated from their relationship with SHSU.

12. The person responsible for the information resource facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

13. The person responsible for the information resource facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

14. Environmental conditions in all data centers will be monitored and protected from environmental threats commensurate with the identified risks and their importance to SHSU mission critical business processes.

15. Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

16. Physical access to all restricted information resource facilities must be documented and managed.

17. All information resource facilities must be physically protected in proportion to the criticality or importance of their function at SHSU.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, June, 2023
Next Review: June, 2024