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

IT Physical Access & Environmental Policy: IT-25

PURPOSE:

This policy is intended to establish standards for securing IT@Sam data centers, network closets and protected IT facilities on the SHSU campuses. 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@Sam data centers are monitored and remediated in a timely manner.

SCOPE:

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

POLICY STATEMENT:

IT@Sam is responsible for the safety and security of data on the SHSU network and the equipment used to run the network infrastructure.

- 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.
- Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all restricted information technology resource facilities must be documented and managed.
- All information technology resource facilities must be physically protected in proportion to the criticality or importance of their function at SHSU.
- Access to information technology resource facilities must be granted only to SHSU support personnel and contractors whose job responsibilities require access to that facility.
- The process of granting card and/or key access to information technology resource facilities must include the approval of the person responsible for the facility.

- Each individual that is granted access rights to an information technology resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements
- Requests for physical access must come from IT@Sam.
- Access cards and/or keys must not be shared or loaned to others.
- 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.
- Lost or stolen access cards and/or keys must be reported immediately to the appropriate department.
- All information technology resource facilities that allow visitor access will track access with a sign in/out log.
- Visitors must be escorted in card access controlled areas of information technology resource facilities.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or not returned.
- Card access records and visitors logs for information technology resource facilities must be kept for routine review based upon the criticality of the information resources being protected.
- The person responsible for the information technology 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.
- The person responsible for the information technology resource facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the information technology 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.
- Restricted access rooms should be identified with discrete signage.

Related Policies, References and Attachments:

An index of approved IT@SAM policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security

Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President's Cabinet, February 6, 2012
Next Review: November 1, 2015