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

Third Party Access Policy: IT-28

PURPOSE:

SHSU receives requests for direct connections to its information technology resources from contractors, vendors and other third parties for support services, contract work or other remote access solutions for the university.

The purpose of this policy is to define standards for connecting to SHSU information technology resources. These standards are designed to minimize the potential exposure to SHSU from damages which may result from unauthorized use of SHSU information technology resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical SHSU internal systems, etc.

SCOPE:

The Third Party Access Policy pertains to all third party organizations and individuals that require access to non-public electronic resources maintained by SHSU.

POLICY STATEMENT:

As a condition of gaining access to SHSU information technology resources:
- Every third-party must sign an SHSU Non-Disclosure Agreement.
- All third parties must be sponsored by an SHSU department, organization or employee.
- All third-party access must be uniquely identifiable and password management must comply with the User Accounts Password Policy (IT-02) and IT Administrator/Special Access Policy (IT-18) guidelines.
- All third-party account holders must provide contact information that will be used to contact them in the event of account status changes, misuse, or termination of the agreement.
- All changes to access granted under this policy must originate from the SHSU sponsor and are subject to a security review.
- Third parties must be made aware and must comply with all applicable SHSU policies, practice standards, agreements and guidelines, including but not limited to:
    - Acceptable Use Policy (IT-03)
    - Encryption Policy (IT-10)
    - Privacy Policy (IT-27)
    - Network Access Policy (IT-12)

- o Portable Computing Policy (IT-26)
  - o Change Management Policy (IT-09)
  - o Information Security Program
- Third-party agreements and contracts must specify:
  - o The SHSU information to which the third party has access.
  - o How SHSU information is to be protected by the third party.
  - o Acceptable methods for the return, destruction or disposal of SHSU information in the third party's possession at the end of the contract.
- Third parties must only use SHSU information and information technology resources for the purpose of the business agreement.
- Any other SHSU information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others.
- Third-party personnel must report all security incidents immediately to the appropriate SHSU sponsor and the Information Security Officer (ISO).

Any third-party account holder that violates this policy will have the account suspended and the account holder's sponsor will be notified.   Following a review, SHSU will implement the actions specified by the ISO to reinstate or remove the account.

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, 2014