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

Virtual Private Network Access Policy: IT-04

PURPOSE:

The Virtual Private Network Access Policy exists to protect SHSU information technology resources. Security of the information technology resources that reside on the SHSU domain is ensured in part through restricting remote access. Virtual Private Network (VPN) allows SHSU users (Regular and Visitor Account users as defined in Policy IT-01) to securely access the university's network via an existing connection to the Internet from a remote location.

Using VPN connections presents an increased security risk if the connecting computer is not secure. Security, Internet access and configuration of the connecting computer are solely the responsibilities of the user account holder making the connection.

SCOPE:

The SHSU Virtual Private Network Access policy applies equally to all individuals with authorized VPN accounts accessing Sam Houston State University information technology resources.

POLICY STATEMENT:

1. It is the responsibility of individuals with VPN privileges to ensure that unauthorized users are not allowed access to the SHSU network using their security credentials.
2. VPN authentication is controlled using SHSU user account credentials.
3. VPN gateways are managed by IT@Sam.
4. All computers connected to the SHSU network via VPN or any other technology must use the most up-to-date anti-virus software regardless of the type or ownership of the device.
5. VPN users will be automatically disconnected from SHSU's network after a designated time out period as determined by IT@Sam. The user must then logon again to reconnect to the network.
6. Pings or other network utilities must not be used to keep the VPN connection open.
7. Users of computers that are not SHSU-owned equipment must configure the equipment in compliance with SHSU policies and procedures.
8. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of SHSU's network, and VPN users must be in compliance with SHSU policies and procedures.

9. VPN access does not guarantee access to all campus systems/applications. Access to systems/applications will be evaluated on a case-by-case basis.

DEFINITIONS:

Unauthorized user: A person who has not been given official permission or approval to access SHSU systems.

Virtual Private Network (VPN): Extends a private network across a public network, like the internet, to provide remote offices or individuals with secure access to the SHSU network using special hardware and software.

VPN Gateway: (Also known as a VPN Router) is a connection point that connects two networks which are connected by a non-secure network such as the Internet.

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 30, 2015
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2016