

**Sam Houston State University**  
**A Member of The Texas State University System**  
**Information Technology**

**Virtual Private Network Access Policy: IT-04**

**PURPOSE:**

The Virtual Private Network Access Policy exists to protect Sam Houston State University (SHSU) information resources. Security of the information resources that reside on the SHSU domain is ensured in part through restricting remote access. Virtual Private Network (VPN) allows eligible SHSU users 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 SHSU 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 Information Technology.
4. All computers connected to the SHSU network via VPN or any other technology, regardless of whether the device is owned personally or by SHSU, must use a secure configuration that includes:
  - a. A supported anti-virus software with up-to-date definitions/rules;
  - b. A hardware or software-based firewall configured to not allow untrusted connections to the device;
  - c. A manufacturer-supported Operating System with the latest security updates installed;
  - d. VPN users will be automatically disconnected from SHSU's network after a designated time out period as determined by Information Technology. The user must then logon again to reconnect to the network.
5. VPN users are not to circumvent VPN session timeouts.
6. VPN access does not guarantee access to all campus systems/applications. Access to systems/applications will be evaluated on a case-by-case basis.

**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, April 11, 2023

Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023

Next Review: April, 2024