SVHEC Opportunity Lives Here

Southern Virginia Higher Education Center
Policy

Policy # 4104
Policy Title: REMOTE NETWORK ACCESS IPSec. [VIRTUAL PRIVATE NETWORK (VPN)] POLICY

Responsible Oversight Director: Chief Finance & Operations Officer (CFOO)

Date of Current Revision or Creation: March 4, 2008

A. PURPOSE

The purpose of this policy is to provide guidelines for establishing a remote network access IPsec. [Virtual Private Network (VPN)] to the Southern Virginia Higher Education Center's (SVHEC) network and establish authorized users of the SVHEC's VPN.

B. AUTHORITY

Virginia Code Section 23-231.24-29, as amended, grants authority to the Board of Trustees to establish rules and regulations for the institution. Section VIII (E) of the Board of Trustees Bylaws grants authority to the Executive Director to implement the policies and procedures of the Board relating to the SVHEC operations.

The policies of the SVHEC fall within the following framework and hierarchy and, therefore, are subject to compliance with laws and regulations instituted by higher levels of authority:

1. Federal laws and regulations
2. State laws and regulations
3. Board of Trustees policies
4. **SVHEC policies**
5. Departmental policies and procedures

In the event of a conflict between different levels in 1 through 5 above, the lower numerical heading shall take precedence over higher numerical heading.

C. DEFINITIONS

Authorized Person - Person who has established a need to VPN to the SVHEC network and received the necessary authorization.

SVHEC Member Owned Device – Computers, telecommunication equipment, and any other computing device that belongs to and is maintained by an official SVHEC member organization [for small organizations without organized IT departments this IT function may be provided by the SVHEC if contracted].

SVHEC Network – Computers, telecommunication equipment, networks (wired or wireless), databases and data processing systems, the SVHEC SharePoint, printing management information systems, and related information, equipment, goods and services.

SCOPE

This policy applies to all colleges and universities offering programs and courses at the SVHEC and those agencies offering services to students of the SVHEC. SVHEC policies and procedures are applicable to all members of the SVHEC community unless a specific policy states otherwise. SVHEC policies are located on the website, www.svhec.org.

D. POLICY STATEMENT

Authorized employees and other approved users of the SVHEC along with authorized employees and other approved users for the SVHEC member organizations with approved equipment may utilize the benefits of the SVHEC's VPN, which is a 'user managed" service. This means that an authorized user is responsible for selecting an Internet Service Provider (ISP), installing any required software, and paying associated fees.

Therefore, authorized users agree to the following:

1. Authorized employees or others will ensure that no unauthorized user is allowed access to the SVHEC's network.

2. VPN access will be controlled by secret passphrase (known to IT network administrators only) and the users SVHEC logon and password [which is kept in accordance with the SVHEC network access policy].

3. When actively connected to the SVHEC's network, VPN will force all traffic to and from the PC over the VPN tunnel; and will handle traffic directed outside the SVHEC network based on the following conditions:

- SVHEC owned device: all other traffic will be routed to the Internet.
- Approved (by SVHEC IT Manager) SVHEC member owned device: all other traffic will be routed to the Internet.
- Approved (by SVHEC's IT Manager and their reporting director) Non-SVHEC owned device (employee owned): all other traffic will be dropped.

4. Dual (Split) tunneling is not permitted unless a written exception is documented and signed by the SVHEC IT Manager and his/her Director.

5. VPN Gateways will be setup and managed by the SVHEC's IT Network Administrators Group only.

6. VPN users will be automatically disconnected from the SVHEC's network after thirty minutes of inactivity and artificial methods like Pings to keep a connection open are considered a violation of this policy.

7. A single VPN connection is limited to a maximum time of 24 hours.

8. Users of computers that do not belong to the SVHEC are required to be configured to comply with the SVHEC's VPN and Network Access Standard.

9. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the SVHEC Network, and as such are subject to the same policies and regulations that apply to computers of the SVHEC, i.e. personal computers must be configured to comply with all SVHEC Security and IT Policies although this exception is rarely granted.

E. RELATED INFORMATION

VPN and Network Access Standard

[1]Procedures are not a part of the policy document. They are maintained separately.

POLICY HISTORY

****

Director Policy Review Committee & Policy Responsible Oversight Director - Approval to Proceed:

Responsible Oversight Director's Signature — 7/1/2013 Date

Executive Director – Provisional Approval of Policy:

Executive Director's Signature — 7/1/2013 Date

Date of Presentation to Board of Trustees:

Date of Approval by Board of Trustees:

Default Approval Date (if necessary):

Board of Trustee – Approval of Policy:

Chairman's or Designee's Signature — Date

Policy Revision Dates: February 24, 2014

Scheduled Review Date: February 2019