

I. Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the Pellissippi State campus network.

II. Scope

This policy applies to all Pellissippi State employees utilizing VPNs to access the Pellissippi State network.

III. Policy

Approved Pellissippi State employees may utilize the benefits of VPNs, which are a user managed service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

- A. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Pellissippi State internal networks
- B. VPN use is to be controlled using a username/password authentication from the Pellissippi State Active Directory.
- C. When actively connected to the campus network, VPNs will force all traffic to and from the PC over the VPN connection.
- D. Dual (split) tunneling is NOT permitted; only one network connection is allowed for users accessing college resources.
- E. All computers connected to Pellissippi State internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the college standard or equivalent; this includes computers owned by the college and computers owned by employees.
- F. VPN users will be automatically disconnected from Pellissippi State's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- G. The VPN concentrator is limited to total connection time of 8 hours per session.
- H. Users of computers that are not Pellissippi State-owned equipment must configure the equipment to comply with Pellissippi State's VPN and Network policies.
- I. Only College-supplied VPN or SSL VPN clients may be used.
- J. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Pellissippi State's network, and as such are subject to the same rules and regulations that apply to Pellissippi State-owned equipment, i.e., their machines must be configured to comply with Pellissippi State's Security Policies.
- K. At no time should any Pellissippi State employee provide their college login or email password to anyone, not even family members.

- L. Pellissippi State employees with remote access privileges must ensure that their Pellissippi State owned or personal computer or workstation which is remotely connected to Pellissippi State's corporate network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- M. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

IV. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, including loss of remote access privileges.

V. Definitions

<u>Term</u>	<u>Definition</u>
VPN	Virtual Private Network, a method for accessing a remote network via tunneling through the internet.
Remote Access	Any access to Pellissippi State's network through a non-Pellissippi State controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Pellissippi State network (such as the internet or a home network) for a remote device (PC, PDA, WAP phone, etc.) while connected into the College network via a VPN tunnel.
Dual	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the College network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Pellissippi State-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Pellissippi State and an ISP, depending on packet destination.

Reviewed/Recommended: President's Staff, March 26, 2007

Approved: President Allen G. Edwards, March 26, 2007

Editorial Changes: June 30, 2010