POLICY 08:13:10
REMOTE ACCESS

I. Purpose

The purpose of this policy is to provide guidelines for Remote Access connections to the Pellissippi State campus network.

II. Scope

This policy applies to all Pellissippi State employees utilizing remote access technologies for connecting to the Pellissippi State network.

Virtual Desktop

The virtual desktop environment is a session-based, non-persistent connection. In other words the virtual desktop will resort back to a default setup after you logout. A user's virtual environment will include the user's h: drive and any departmental drive or other shared drives that the user normally has access to on campus. Any files placed on the virtual c: drives are not saved. The virtual desktop environment is not a workstation replacement because the available software is limited to core applications, such as Internet Explorer and Microsoft Office. The virtual desktop environment is provided to faculty and staff who are not prohibited by contract from working from home.

Virtual Private Network

Virtual Private Network (VPN) is a method for accessing a remote network via tunneling through the internet. This is a user managed service, which means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Pellissippi State internal networks. When actively connected to the campus network, VPNs will force all traffic to and from the PC over the VPN connection.

III. Policy

Remote Access use is controlled using a username/password authentication from the Pellissippi State Active Directory. All other related Data System Use Policies, including but not limited to the following, are in full effect and enforced with using remote access.

http://www.tbr.edu/policies/default.aspx?id=4862 (Information Technology Resources)
http://www.pstcc.edu/ppm/pdf/08-13-01.pdf (Microcomputer Usage)
http://www.pstcc.edu/ppm/pdf/08-13-02.pdf (Computer Account Policy)
http://www.pstcc.edu/ppm/pdf/08-13-05.pdf (Computer System Use)
http://www.pstcc.edu/ppm/pdf/08-13-08.pdf (Electronic Account Access)
http://www.pstcc.edu/ppm/pdf/08-13-09.pdf (Wireless Network Policy)

Unauthorized use of the remote access technologies may result in administrative, disciplinary, and/or legal actions. Pellissippi State reserves the right to view, monitor, and/or record activity with the

virtual desktop environment without notice. Any information obtained by monitoring, reviewing, and/or recording may be subject to review by the appropriate authorities.

IV. End User Responsibilities

1. By using Pellissippi State log-on credentials, the user is certifying that he or she is not knowingly posing a threat to the College's network directly or through the virtual desktop environment. These threats include but are not limited to viruses, malware, spyware, key logging, or other types of threats that may divulge personal information or company information and/or reduce the performance of network resources.

2. The user agrees not to transfer and/or record personal identifiable information from the Pellissippi State network on the user's personal machine. The user agrees to follow the laws and policies including but not limited to those in place within the United States of America, the State of Tennessee, and/or Pellissippi State. These laws and policies include but are not limited to the following:

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g; 34 CFR Part 99) - information and resources to ensure compliance with FERPA for on-campus units that must protect the privacy of student education records.

Gramm-Leach Bliley Act (GLB) - information and resources intended to help ensure compliance with the "Gramm-Leach-Bliley Act" or GLB Act for on-campus units handling students' personal financial information.

Health Insurance Portability and Accountability Act (HIPAA) - information and resources intended to help ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) for on-campus units handling electronic protected health information (ePHI).

3. The user is responsible for obtaining timely and appropriate approval for use of the remote access environment from his or her vice president at Pellissippi State.

4. The user is responsible for timely and appropriate notification to Pellissippi State of any breach or possible breach in security, policy, or law that may have occurred while using the remote access environment.

5. With VPN access, only one network connection is allowed for users accessing college resources; dual (split) tunneling is not permitted.

6. 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.

7. VPN users will be automatically disconnected from Pellissippi State's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open. The VPN concentrator is limited to total connection time of 8 hours per session.

8. Users of computers that are not Pellissippi State-owned equipment must configure the equipment to comply with Pellissippi State's VPN and network policies. Only college-supplied VPN or SSL VPN clients may be used.

9. At no time should any Pellissippi State employees provide their college log-in or email password to anyone, not even family members.

10. 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.

11. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

V. Enforcement, Termination of Access and Changes to Terms

Any employee found to have violated this policy may be subject to disciplinary action, including loss of remote access privileges. Pellissippi State reserves the right at any time to deny access to the virtual desktop environment or any portion thereof. Pellissippi State may change these restrictions and conditions at any time, and all users will be subject to the terms and conditions in effect at the time they are using or attempting to use the virtual desktop environment.

VI. Definitions

Term	**Definition**
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
Editorial Changes: June 25, 2012
Reviewed/Recommended: President's Council, March 31, 2014
Approved: President L. Anthony Wise, Jr. March 31, 2014