

I. Purpose

The purpose of this policy is to provide guidelines for providing and revoking remote access connections to the Pellissippi State campus network and to College-owned or -provided technology, resources and data. This policy expands Pellissippi State Policy 08:13:01 - Information Technology Acceptable Use by including specific direction regarding remote access.

II. Scope and Applicability

This policy applies to all Pellissippi State employees utilizing remote access technologies for connecting to the Pellissippi State network. Remote Access is limited to employees of the College. The virtual desktop environment may be provided to faculty and staff who are working from home. Information Services staff shall be responsible for providing services within the scope of this policy.

III. Definitions

Remote Access - Any access to Pellissippi State's network through a non-Pellissippi State controlled network, device, or medium.

Virtual Desktop - The virtual desktop environment is a session-based, non-persistent connection that will resort back to a default setup after you logout.

Virtual Private Network (VPN) - an encrypted connection over a less secure network, such as the public internet while maintaining privacy through security procedures and tunneling protocols which encrypt data at the sending end and decrypt it at the receiving end. This creates a "tunnel" that cannot be entered by data that is not properly encrypted

IV. Risks, Liabilities and Disclaimers

The College makes available remote access to campus resources to approved employees and provides technical support to College-owned equipment and accounts. The College accepts no responsibility for any loss of data or damage to data or services arising directly or indirectly from the use of these systems and resources or for any consequential loss or damage. The College makes no warranty, express or implied, regarding the services offered or their fitness for any particular purpose.

Use of remote access signifies the following:

- The user agrees to comply with the provisions of this Remote Access Policy and all other applicable policies
- The user accepts responsibility for knowing the contents of this policy statement. Failure to read or acknowledge this statement will not be an excuse for noncompliance.

- The user accepts that failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action.

V. Policy and User Responsibilities

Policy

Pellissippi State Community College is responsible for providing a secure and reliable campus network to ensure the confidentiality, integrity, and availability of technology and data. This is accomplished through the development and implementation of compliance standards which address security requirements and expectations for acceptable use of computer systems, including the remote access to the campus network.

Remote Access use is granted only by approval of an employee's supervisor and the appropriate vice president. The remote access compliance form must be completed before access is granted. The form can be provided by contacting the HelpDesk or downloading it from the Information Services Service Catalog site.

Remote Access is only provided to an individual employee account. Access is controlled using a username/password authentication from the Pellissippi State Active Directory.

Remote access to the college network is granted via the use of virtual desktop or a College-provided network access point that will require hardwire connection to a user's personal network. This access point will be assigned and monitored directly by the College's networking technical support, who will have the ability to work with end users and access the connection up to but not past the remote access point.

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 standard virtual desktop environment is not a workstation replacement because the available software is limited to core applications, such as web browsers and Microsoft Office.

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.

All other related information technology system use policies, including but not limited to the following, are in full effect and enforced with using remote access.

- 08:13:01 Information Technology Acceptable Use
- [08:13:02 Computer Account](#)
- [08:13:06 Bring Your Own Device \(BYOD\)](#)
- [08:13:08 Electronic Account Access](#)
- [08:13:09 Wireless Network](#)
- TBR Policy 1.08.0.0 [Information Technology Resources](#)

B. End User Responsibilities

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.

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.

The user agrees not to transfer and/or record confidential or restricted 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).

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.

All computers connected to Pellissippi State internal networks via or any remote access 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. Employees who use personally owned devices to connect remotely to the college's network must also comply with [Pellissippi State Policy No. 08:13:06 Bring Your Own Device \(BYOD\)](#).

At no time should any Pellissippi State employees provide their college log-in or email password to another user.

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.

VI. Enforcement

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.

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

Reviewed/Recommended: President's Council, September 9, 2019

Approved: President L. Anthony Wise, Jr., September 9, 2019