Policy Title: Virtual Private Network (VPN)

Policy Type: Technology **New/revised:** Revised

Old Policy #: Virtual Private Network (VPN)

Approval level: ☐ Board of Trustees
☒ President
☐ Vice President
☐ Other (specify here)

Purpose: The purpose of this policy is to state the requirements for remote access to computing resources hosted at ETSU using remote access technologies.

Policy:

Introduction

In order to access computing resources hosted at East Tennessee State University from off campus, use of ETSU remote access services is required. A remote access connection is a secured private network connection built on top of a public network, such as the Internet. Remote access provides a secure, encrypted connection, or tunnel, over the Internet between an individual computer (such as a computer off campus) and a private network (such as ETSU's). Use of remote access allows authorized members of the ETSU community to securely access ETSU network resources as if they were on the campus.

Remote access connections allow an outside computer to connect directly to the University's network. This arrangement provides convenience for the remote worker, but bypasses any firewall restrictions that may be in place. There is a network security risk present when accessing the university's network from an outside source. This risk is particularly pronounced for remote access connections from privately owned computers, as the University cannot ensure the computer has sufficient protection configured (e.g. anti-virus, anti-spyware). The risk posed by ETSU-owned computers is still present, but to a lesser degree.

Responsibilities

Information Technology Services (ITS) is responsible for implementing and maintaining the University's remote access services. Therefore, ITS is also responsible for activities relating to this policy. Accordingly, ITS will manage the configuration of the University's remote access service.

Approved Remote Access Clients

ETSU currently implements two separate remote access solutions:

- Microsoft Remote Desktop Gateway (RDG):
    - Allows you to log in to your ETSU computer from off-campus
    - Requires no software installation

    - Presents a lower security risk
    - Does not expire (subject to periodic review)
- Cisco AnyConnect (VPN):
    - Allows you to connect to the ETSU network from off-campus
    - Requires software installation
    - Presents a higher security risk
    - Expires, at minimum, every 12 months

Microsoft Remote Desktop Gateway (RDP) is the recommended choice for most remote access users. This option provides sufficient access for the majority of users and reduces security risks to the university.

Policy for Remote Access

ETSU employees, and authorized third parties (customers, vendors, etc.) may, under some circumstances, utilize remote access to access ETSU computing resources for which they have been granted access.

Regular, full-time ETSU faculty or staff employees that have a valid ETSU Domain User Account may request remote access to the ETSU network by completing a Remote Access Request Form. A letter of justification must accompany the request. The letter should address, in sufficient detail, what resources will be accessed through the VPN and explanation for why the resources cannot be accessed through conventional means. Requests omitting a letter of justification will be returned to the requester as incomplete.

With the exception of Remote Desktop Gateway (see Operational Procedures section) remote access is valid for a set period of time. Requesters should indicate the date remote access should take effect and the date access should expire. Remote access may be granted for a period of up to twelve months, after which remote access for the account will expire. Requesters will be notified via phone or email approximately thirty (30) days before remote access expires. Account holders may resubmit a Remote Access Request Form up to thirty (30) days before the remote access expiration date to continue remote access without disruption.

Guidelines for Access:

- Faculty and Administrative accounts may be granted remote access.
- Vendor Accounts may be granted remote access. Vendor accounts are setup specifically for vendors to access ETSU resources for support purposes. Vendor accounts must be sponsored by an ETSU employee. The account sponsor bears responsibility for the account and its use by the vendor. If the vendor account does not already exist, a request to establish one must be made at the same time remote access is requested.
- Departmental Accounts will not be granted remote access due to lack of accountability. These accounts are typically shared among several users and it is difficult to trace a specific user back to the account at any given time.
- Temporary Accounts will not be granted remote access.
- Student accounts will not be granted remote access.

- Clerical or Support accounts will not be granted remote access without prior telecommuting approval (Vice President endorsement required).

All remote access account holders are subject to the following Remote Access Terms of Use.

Remote Access Terms of Use

Any user found to have violated the following terms of use may be subject to loss of privileges or services and other disciplinary action.

1. It is the responsibility of all ETSU employees and authorized third parties with remote access privileges to ensure that unauthorized users are not allowed access to internal University networks and associated content.
2. All individuals and machines, including university-owned and personal equipment, are a de facto extension of ETSU's network, and as such are subject to the university's Acceptable Use Policy.
3. All computers connected to ETSU's internal network via remote access or any other technology must use a properly configured, up-to-date operating system and anti-virus software; this includes all personally-owned computers.
4. Redistribution of the ETSU remote access installers or associated installation information is prohibited.
5. All network activity during a remote access session is subject to ETSU policies.
6. All users of the ETSU remote access services shall only utilize resources for which they have been granted permission and rights to use.

Operational Procedures

In order to use remote access, users will need a connection to the Internet from their off-campus location. While dial-up Internet connections may utilize a remote access connection, performance is very slow and is not recommended or supported.

- Remote access users will be automatically disconnected from the ETSU network after 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open are prohibited.
- Information Technology Services will only provide support for approved remote access software clients.
- Questions related to the use of ETSU remote access should be directed to the ITS Help Desk at 423-439-4648 or itshelp@etsu.edu .

Policy Dispute

The Chief Information Officer is charged with the responsibility to periodically review this policy and propose changes as needed.

Notes:

Approved: Information Technology Governance Council
Reviewed: February 2017

3/24/2017 – approved by the Board of Trustees.