EAST TENNESSEE STATE
UNIVERSITY

Remote Access

Policy Effective Date: 3/24/2017 • **Policy Revised:** Insert
Procedures Effective Date: 3/24/2017 • **Procedures Revised:** Insert

Policy Name: Remote Access

Policy Purpose

This policy specifies requirements for inbound remote connection to the ETSU network from any host device (mobile devices, tablets, laptops). These rules and requirements minimize the potential for unauthorized access to ETSU resources.

Applicability

This policy is applicable to employees and third-party vendors.

Responsible Official, Office, and Interpretation

The Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer, in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Authorized User

An individual who has been granted explicit permission to access the ETSU network, systems, or resources based on their role, responsibilities, and credentials.

Departmental Account

Departmental Accounts function similarly to ETSU faculty and staff user accounts. They are fully licensed Microsoft accounts that can be used to sign in to ETSU computers, connect to ETSU Wi-Fi, and access both the locally installed and web-based versions of Office 365.

Pings

A network utility to test connectivity between two devices or systems, such as a remote user's device and ETSU servers or network.

Remote Access

A secure, encrypted connection or tunnel over the internet between an individual computing device and a private network. Remote Access allows Authorized Users to securely access ETSU network resources from a device that is not on the ETSU network.

Remote Access Connection

A secured private network connection built on top of a public network, such as the internet.

Sponsor

The ETSU employee requesting Remote Access to university resources on behalf of a third-party company or individual.

Policy Name: Remote Access

Policy

It is the responsibility of employees with approved Remote Access privileges to the ETSU network to ensure that their Remote Access Connection is treated as an on-site connection. Access to the ETSU network is limited to Authorized Users. When accessing the ETSU network from personal devices, Authorized Users are responsible for preventing access by non-authorized individuals.

Illegal activities on the ETSU network by any user are prohibited. Authorized Users bear responsibility for, and the consequences of, misuse of their access. For further information and definitions, see the Acceptable Use of Information Technology Resources Policy.

1. Terms of Use.

All individuals and devices, including ETSU-owned and personal equipment, are considered a de facto extension of ETSU's network, and are therefore subject to the Acceptable Use of Information Technology Resources policy. All ETSU-owned and personal computing devices connected to ETSU's network via Remote Access must use a properly configured, updated operating system and anti-virus software.

All network activity during a Remote Access session is subject to university policies. All users of Remote Access services may only access resources for which they have been granted permission.

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

2. Authorized Access Eligibility.

All users who require Remote Access must complete a Remote Access Request Form. Requestors must enter a valid business purpose for Remote Access to ETSU resources. Requestors must also review and acknowledge the Acceptable Use of Information Technology Resources, Remote Access, and Telecommuting policies before submitting the form. Annual renewal is required to maintain Remote Access. Remote Access privileges will only be assigned if the requestor has successfully completed the current Cybersecurity Awareness Training.

2.1. User Eligibility.

2.1.1. Regular, full-time employees may be granted Remote Access upon submission of the request form and after receiving approval from their direct supervisor and dean or vice president.

2.1.2. Third-party vendor and contractor accounts may be granted Remote Access for specific support purposes. Requests for third party Remote Access must be completed by an ETSU Sponsor. The Sponsor bears the responsibility for any activity occurring while the third party is accessing the network remotely.

2.1.3. Departmental Accounts are not eligible for Remote Access privileges due to a lack of accountability.

2.1.4. Temporary employees are not eligible for Remote Access privileges.

2.1.5. Students are not eligible for Remote Access privileges.

Outbound Remote Access Connections to other networks from the ETSU network are prohibited.

3. Remote Access Operations.

Remote Access services are only accessible from off-campus. Authorized Users will not be able to connect remotely while on the ETSU network. Remote Access Connections will be automatically disconnected after 30 minutes of inactivity. The Authorized User must repeat the login process when the connection is broken. Pings or other artificial network processes to maintain the connection are prohibited.

Authorized Users must have a secure and reliable connection to the internet from their off-campus location.

Information Technology Services (ITS) will only provide support for approved Remote Access software clients. ITS cannot troubleshoot issues involving the user's home network or personal computing device. ITS personnel cannot travel to the user's off-campus location. Limited support may be provided in person at the ITS Help Desk for personal computing devices.

4. Exceptions.

Any exceptions to this policy must be requested by submitting a detailed written request with justification to its@etsu.edu. The Chief Information Officer or designee will review and approval. The decision of the Chief Information Officer is final.

5. Approved Remote Access Clients.

Approved users may establish Remote Access Connections to the ETSU network using either Microsoft Remote Desktop Gateway (RDG), Cisco AnyConnect, or Microsoft Global Secure Access.

Procedures

N/A

Applicable Forms and Websites

Remote Access Request Form

Authority and Revisions

Authority: N/A

Previous Policy: Virtual Private Network (VPN)

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational programs and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.