Remote Access Policy

The purpose of this policy is to define standards for connecting to the St. Thomas network from remote devices. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of university resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

This policy is guided by the following objectives:

1. Preserve St. Thomas' ability to operate and maintain ITS Resources
2. Protect the security and functionality of university ITS Resources and the data stored on those resources
3. Safeguard the privacy, property, rights, and data of users of university ITS Resources
4. Preserve the integrity and reputation of the University
5. Comply with applicable federal, state, and local laws
6. Comply with applicable university policies, standards, guidelines, and procedures

Responsibilities

The division of Information Technology Services is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Associate Vice President of Information Security & Risk Management, CISO or delegate is the responsible officer.

Scope

This policy applies to all University employees and affiliates including vendors and agents with a university owned or personally-owned devices used to connect to the St. Thomas network. This policy applies to remote access connections used to do work on behalf of St. Thomas or for University related business. Remote access includes all direct connections to university systems and networks from outside of the St. Thomas network.

University of St. Thomas faculty or staff having a valid St. Thomas username may request Virtual Private Network (VPN) access to the St. Thomas network by consulting with their technology consultant. The VPN includes hardware and/or software technology used to provide secure access to the university network.

VPN Terms of Use

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

1. It is the responsibility of all St. Thomas employees and authorized third parties with VPN privileges to ensure that unauthorized users are not allowed access to internal University networks and associated content. At no time should any St. Thomas employee provide their username or password to anyone, not even family members.
2. All network activity during a VPN session is subject to St. Thomas policies. All individuals and machines, while using St. Thomas' VPN technology, including university-owned and personal equipment, are a de facto extension of St. Thomas network, and as such are subject to the University's Responsible Use Policy.
3. All existing university policies related to data standards, data privacy, and confidentiality should be followed when connecting to university systems remotely and/or via the VPN.
4. All devices connected to the St. Thomas internal network via the VPN or any other technology must use a properly configured, up-to-date operating system and anti-virus software; this includes all personally-owned devices. Antivirus software is available for St. Thomas faculty and staff.

Guidelines for Access

- Remote access to the St. Thomas network is only allowed via a VPN connection, or through approved designated secure terminal services.
- It is the responsibility of St. Thomas employees or affiliates with remote access privileges to the university network to ensure that their remote access connection is given the same consideration as the user's on-site connection. Please review St. Thomas computing policies located the Responsible Use Policy webpage.
- Generic accounts shall not be granted VPN access due to lack of accountability. These accounts are typically shared among several users and there is no way to trace a specific user back to the account at any given time.
- Student accounts shall not be granted VPN access.
- Vendor accounts may be granted VPN access on a case by case basis. Vendor accounts are setup specifically for vendors to access St. Thomas resources for support purposes. Vendor accounts must be sponsored by a St. Thomas 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 VPN access is requested.
- All VPN account holders are subject to the VPN Terms of Use. In order to use the VPN, you need a connection to the Internet from your off-campus location. Dialup Internet connections are not supported.
- In order to access the St. Thomas VPN your device will need to meet the System Requirements for VPN usage defined on the Working Remotely Website.
- Device specific performance is not guaranteed.

- VPN users will be automatically disconnected from the St. Thomas network after a period of inactivity. Save your work often.
- Only resources hosted by St. Thomas (such as Banner and Cognos) are secured by the VPN. Other resources accessed during a VPN session (such as Facebook, CNN, Google Mail) are not secured by the St. Thomas VPN.
- Exceptions to this policy will be handled on a case by case basis.

If you have any questions related to the use of the St. Thomas VPN, please contact the Tech Desk at (651) 962-6230.