REMOTE ACCESS POLICY

April 2008

TNS –POL - 013

PURPOSE

The purpose of this policy is to define standards for the usage and establishing a secure remote access to computing resources hosted at Southern University using Virtual Private Network (VPN). These standards are designed to minimize any security adversity that may cause any potential damage to Southern University network or assets from which may result from unauthorized use of the University's resources.

DEFINTION

What is a Virtual Private Network (VPN)?

In order to access computing resources hosted at Southern University from off-campus, use of our Virtual Private Network (VPN) is required. A VPN is a secured private network connection built on top of a public network, such as the Internet. A VPN provides a secure encrypted connection or tunnel over the Internet between an individual computer and a private network. Use of a VPN allows authorized members of Southern University to securely access the University network resources as if they were on the campus.

Who can use the VPN?

Only authorized Southern University staff and authorized third parties (customers, vendors, etc.) may utilize the benefits of the VPN to access computing resources to which they have been granted access. In order to use the VPN, you need a connection to the Internet from your off-campus location. The University does not provide you with an off campus internet connection, your Internet Service Provider does. While dialup Internet connections can utilize a VPN connection, performance is very slow and is not recommended or supported. To see if you are allowed VPN access, contact personnel of IT Security.

SCOPE

This policy applies to all authorized users with a University owned or personally owned computer or workstation used to connect to the Southern University network through VPN. This policy applies to remote access connections used to do work on behalf of Southern University, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, and etc.

POLICY AND PROCEDURES

1. It is the responsibility of all authorized users with VPN privileges to ensure that unauthorized users are not allowed access to internal University networks and computing resources.

2. **All** individuals and computers, while using the University’s VPN, including university-owned and personal equipment, are an effective extension of Southern University's network, and as such are subject to the University's Acceptable Use Policy.

3. **All** computers, University-owned and personally-owned, connected to the University's internal network via the VPN or any other technology must use a properly configured up-to-date operating system and configured up-to-date anti-virus software.

4. Redistribution of the University’s VPN Installer or associated installation information is prohibited.

5. All network activity during a VPN session is subject to the University’s policies.

6. All authorize users of the University’s VPN will only connect to or gain access to machines and resources that they have permission and rights to use.

7. Please review the following policies for details for protecting information when accessing the corporate network via remote access methods, and acceptable use of Southern University's network:

a. TNS Acceptable Use Policy
b. Personal Computing Policy
c. Antivirus Policy
d. Password Policy
e. Authentication Policy

RESPONSIBILITIES

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication with your SU Username and password.

2. Any Southern University employee or contractor who wishes to access any internal computing resource using remote access must obtain approval and authorization from IT Security.

3. At no time should any Southern University employee provide their SU username and password or email to anyone, not even family members.

4. Southern University employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to Southern University’s network, is not connected to any other network at the same time.

5. Southern University employees and contractors with remote access privileges to Southern University’s network **must** use their SU username and password to conduct Southern University business, thereby ensuring that official business is never confused with personal business.

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

7. All hosts that are connected to Southern University internal networks via remote access **must** use a properly configured up-to-date anti-virus software and operating system, this includes personal computers.

8. Blackberry/PDA devices and “smart phones”, due to their fast-paced technological advances are not within the scope of this policy.