II.C.4. Policy: Southeastern Technical College Remote Access

1.0 Purpose
The purpose of this policy is to define standards for connecting to STC's network from any host. These standards are designed to minimize the potential exposure to STC from damages which may result from unauthorized use of STC resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical STC internal systems, etc.

2.0 Scope
This policy applies to all STC employees, students, contractors, vendors and agents with a STC-owned or personally-owned computer or workstation used to connect to the STC network. This policy applies to remote access connections used to do work on behalf of STC or for STC academic courses, 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, Remote Lab Access (RLA), Information Delivery System (IDS), etc.

3.0 Policy
3.1 General

1. It is the responsibility of STC employees, students, contractors, vendors and agents with remote access privileges to STC's multi-campus network to ensure that their remote access connection is given the same consideration as the user's on-site connection to STC.

2. General access to the Internet for recreational use by immediate household members through the STC Network on personal computers is not permitted.

3. Please review the following policies for details of protecting information when accessing the multi-campus network via remote access methods, and acceptable use of STC's network:

   a. *Computer Use Policy*

   b. *Email Use Policy*

   c. *Privacy Notice to Computer Users*

4. For additional information regarding STC's remote access connection options, including how to request service and obtain technical support go to the STC Information Technology Department website.

3.2 Requirements

1. At no time should any STC employee, student, contractor, vendor or agent with remote access privileges provide their login or email password to anyone, not even family members.

2. Routers for dedicated ISDN lines configured for access to the STC network must meet minimum authentication requirements of CHAP.

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

4. Frame Relay must meet minimum authentication requirements of DLCI standards.

5. Non-standard hardware configurations must be approved by the Information Technology Department, and the IT Department must approve security configurations for access to hardware.

6. All hosts that are connected to STC internal networks via remote access technologies must use up-to-date anti-virus software (http://www.southeasterntech.edu/it/virus_info.asp), this includes personal computers.

7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the STC production network must obtain prior approval from the Director of Information Technology.

4.0 Enforcement Abuse or misuse of computing/information technology services may violate this policy, but it may also violate criminal statutes. Therefore, STC will take appropriate action in response to user abuse or misuse of computing/information technology services. Action may include, but not necessarily limited to, the following:

1. Suspension or revocation of computing privileges. Access to all computing facilities and systems can, may, or will be, denied;

2. Reimbursement to Southeastern Tech for resources consumed;

3. Other legal action including action to recover damages;

4. Referral to law enforcement authorities;

5. Computer users (faculty, staff and/or students) will be referred to the appropriate office for disciplinary action.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a <Company Name>-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into <Company Name> and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to STC's multi-campus network through a non-

	STC controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-STC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into STC's multi-campus network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.