Stony Brook University
Computer Science

Remote Access Policy

CS Department Remote Access Policy

1.0 Purpose

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

2.0 Scope

This policy applies to all SUNY Stony Brook CS department users, contractors, vendors and agents with a SUNY Stony Brook CS department-owned or personally-owned computer or workstation used to connect to the SUNY Stony Brook CS department network. This policy applies to remote access connections used to do work on behalf of SUNY Stony Brook CS department, including reading or sending email, class assignments, research projects 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, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of SUNY Stony Brook CS department users, contractors, vendors and agents with remote access privileges to SUNY Stony Brook CS department's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SUNY Stony Brook CS department.
2. General access to the Internet for recreational use by immediate household members through the SUNY Stony Brook CS department Network on personal computers is permitted for faculty. The SUNY Stony Brook CS department faculty is responsible to ensure the family member does not violate any SUNY Stony Brook CS department policies, does not perform illegal activities, and does not use the access for outside business interests. The SUNY Stony Brook CS department employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of SUNY Stony Brook CS department's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding SUNY Stony Brook CS department's remote access connection options, including troubleshooting, etc., go to the Remote Access Service FAQ on the CS department website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced by public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any SUNY Stony Brook CS department user provide their login or email password to anyone, not even family members.

3. SUNY Stony Brook CS department users and contractors with remote access privileges must ensure that their SUNY Stony Brook CS department-owned or personal computer or workstation, which is remotely connected to SUNY Stony Brook CS department's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. Home networks should be protected by a router with NAT and access control enabled.
4. SUNY Stony Brook CS department employees and contractors with remote access privileges to SUNY Stony Brook CS department's network must not use non-SUNY Stony Brook CSdepartment email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SUNY Stony Brook CS department business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the SUNY Stony Brook CS department network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by the CS department systems staff and must approve security configurations for access to hardware.
9. All hosts that are connected to SUNY Stony Brook CS department internal networks via remote access technologies must use the most up-to-date anti-virus software (Downloadable from the CS dept web site), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to SUNY Stony Brook CS department's networks must meet the requirements of SUNY Stony Brook CS department-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the SUNY Stony Brook CS department production network must obtain prior approval from the CS department systems staff.

4.0 Enforcement

Any user found to have violated this policy may be subject to 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 CS department network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a SUNY Stony Brook CS department-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into SUNY Stony Brook CS department 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.
NAT	Network Address translation/ A method to translate internal IP addresses to one or more external IP addresses. This technique also serves to obscure internal host and network configurations.
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 SUNY Stony Brook CS department's network through a non- SUNY Stony Brook CS department controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-SUNY Stony Brook CS department network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into SUNY Stony Brook CS department's network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History