

Information Services and Technology Remote Access Policy

I. PURPOSE

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

II. APPLICABILITY

This policy applies to all UMDNJ employees, students, contractors, vendors and agents with a UMDNJ-owned or personally-owned computer or workstation used to connect to the UMDNJ network. This policy applies to remote access connections used to do work on behalf of UMDNJ, including reading or sending email and viewing intranet web resources.

III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall insure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

IV. DEFINITIONS

- A. 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.
- B. CHAP - Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data 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.
- C. 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.
- D. Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the University network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a UMDNJ-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into UMDNJ and an ISP, depending on packet destination.

- E. 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).
- F. 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.
- G. 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.
- H. Remote Access - Any access to UMDNJ's network through a non-UMDNJ controlled network, device, or medium.
- I. Split-tunneling - Simultaneous direct access to a non-UMDNJ network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into UMDNJ's network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

V. POLICY

General

- A. It is the responsibility of UMDNJ employees, students, contractors, vendors and agents with remote access privileges to UMDNJ's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UMDNJ.
- B. No one other than UMDNJ authorized personnel is allowed the use of UMDNJ's networks. UMDNJ authorized personnel bears the responsibility and consequences should the access be misused.
- C. Please review the following policies for details of protecting information when accessing the university network via remote access methods, and acceptable use of UMDNJ's network:
 1. *Acceptable Encryption Policy*
 2. *Virtual Private Network (VPN) Policy*
 3. *Wireless Communications Policy*
 4. *Acceptable Use Policy*
- D. For additional information regarding UMDNJ's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

Requirements

- A. Secure remote authentication must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases and VPN tunnels in conjunction with password databases. For information on creating a strong pass-phrase see the Password Policy.
- B. At no time should any UMDNJ employee provide their login ID's and/or password(s) to anyone, not even family members.
- C. UMDNJ employees and contractors with remote access privileges must ensure that their UMDNJ-owned or personal computer or workstation, which is remotely connected to UMDNJ'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.
- D. UMDNJ employees and contractors with remote access privileges to UMDNJ's network must not use non-UMDNJ email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to

conduct UMDNJ business, thereby ensuring that official business is never confused with personal business.

- E. Routers for dedicated ISDN lines configured for access to the UMDNJ network must meet minimum authentication requirements of CHAP.
- F. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- G. Frame Relay must meet minimum authentication requirements of DLCI standards.
- H. Non-standard hardware configurations must be approved by IS&T, and IS&T must approve security configurations for access to hardware.
- I. All hosts that are connected to UMDNJ internal networks via remote access technologies, must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
- J. Personal equipment that is used to connect to UMDNJ's networks must meet the requirements of UMDNJ-owned equipment for remote access.
- K. Organizations or individuals who wish to implement non-standard Remote Access solutions to the UMDNJ production network must obtain prior approval from IS&T.

VI. NONCOMPLIANCE AND SANCTIONS

Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action. Under applicable University policies and procedures up to and including termination; civil litigation; and/or criminal prosecution under applicable state and federal statutes.