# LOUISIANA COMMUNITY & TECHNICAL COLLEGE SYSTEM
# Policy # 7.004

## Title: REMOTE ACCESS POLICY

| | | |
|---|---|---|
| Authority: Board Action | Original Adoption: | 08/10/2005 |
| | Effective Date: | 04/08/2009 |
| | Last Revision: | 04/08/2009 |

### Purpose

To define standards for connecting to the Louisiana Community and Technical College (LCTCS) network from any host. These standards are designed to minimize the potential exposure to LCTCS from damages that may result from unauthorized use of LCTCS resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, or damage to critical LCTCS internal systems.

### Scope

This policy applies to all LCTCS employees, contractors, vendors and agents with a LCTCS-owned or personally-owned computer or workstation used to connect to the LCTCS network. This policy applies to remote access connections used to do work on behalf of LCTCS, 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, and cable modems.

### Policy

*General*

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

Remote access usage shall not:

1. Violate any LCTCS policies
2. Perform illegal activities,
3. Be used for outside business interests.

End-users interested in obtaining remote access privileges should contact the LCTCS IS Division through their local IT supporter. Each request for remote access will be evaluated on

a case-by-case basis.

*Requirements*

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication with strong pass-phrases.

2. At no time should any LCTCS employee provide login or email password to anyone, not even family members.

3. With the exception of personal networks that are under the complete control of the user, LCTCS employees and contractors with remote access privileges must ensure that their LCTCS-owned or personal computer or workstation when remotely connected to LCTCS's corporate network is not connected to any other network at the same time.

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

5. All hosts connected to LCTCS internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.

## Support Responsibilities

*College/End-User:*

Provides **first level** support for the desktop, any local area network, or third party networks used to enter LCTCS/college sites and utilize applications via remote access methods.

*LCTCS:*

Provides second level support problem determination for VPN connections. The Security Administrator receives the VPN forms and make sure that all signatures are in place and then submits a help desk ticket to the third party hosting operation.

*Third Party Hosting Operation:*

Provides third level support for VPN connection issues to LCTCS Servers. The vendor creates, and deletes user accounts for VPN users once a help desk ticket has been submitted by the LCTCS Security Administrator requesting action.

## Enforcement

Any employee found to have violated this policy shall have remote access rights revoked and may be subject to disciplinary action, up to and including termination of employment. Restoration of remote access rights will occur on a case-by-case basis in consultation with the employee's supervisor and other authorities as needed.

## Definitions

*Cable Modem*
Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable.

*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 LCTCS- provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into LCTCS and an ISP, depending on packet destination.

*Digital Subscriber Line (DSL)*
A form of high-speed Internet access competing with cable modems.

*Frame Relay*
A method of communication that incrementally can go from the speed of an ISDN to the speed of a Tl line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

*Integrated Services Digital Network (ISDN)*
There are two flavors of Integrated Services Digital Network or ISDN: BRIand PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling information.

*Remote Access*
Any access to LCTCS's corporate network through a non-LCTCS controlled network, device, or medium.

*Secure Shell (SSH)*
A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

*Split-Tunneling*
Simultaneous direct access to a non-LCTCS network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into LCTCS's corporate network via a VPN tunnel.

*Virtual Private Network (VPN)*

A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.