LORD FAIRFAX COMMUNITY COLLEGE
YOUR FUTURE. OUR FOCUS.

Policy No.	70002
Effective Date	2/12/2006
Revision Date	
Revision No.	
Approved:	John J. Sygielski
Date:	February 12, 2006

Technology Services Department
Remote Network Access Policy

1.0 Purpose

This policy provides guidance to faculty, staff, and administration for establishing and supporting remote connections to the College's computer network and related systems. This policy is designed to provide maximum access to information technology resources in place at the College, and to minimize potential exposure to the College from damages that may result from unauthorized use of those resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

2.0 Revision History

Policy updated to reflect new template style. No changes made to original content or wording other than section headings.

3.0 Applicability

This policy applies to all instances where an employee or contractor of the College requires access to College resources from a computer not located on the College's network. Remote access implementations that are covered by this document include, but are not limited to the following: Dial-in Modems, DSL and Cable Modems using VPN or SSL connections.

4.0 Policy

Email - All email accounts are automatically established with remote access capabilities safeguarded by a digital certificate/SSL technology. Email account holders may access their email using a standard web browser. No additional request is necessary to access your email account remotely

VPN - Access to the College's standard desktop applications and to the user's network drives via Microsoft Terminal Services may be requested by completing a Remote Network Access Request form (Attachment A); select Terminal Services on the form. This access will require that the requestor install Cisco Systems VPN (Virtual Private Network) Client in addition to enabling and configuring Microsoft Remote Desktop Connection software on their remote computer.

Desktop - In cases where one or more unique applications are available on the employee's desktop computer only, the user may complete a Remote Network Access Request form; select Direct Connection to Office Desktop on the form. This access will require that the requestor install Cisco Systems VPN (Virtual Private Network) Client in addition to enabling and configuring Microsoft Remote Desktop Connection software on their remote computer. In addition the Technology Services Department will need to configure Microsoft's Remote Desktop Services on the requestor's office desktop computer.

Management - Remote access gateways will be set up and managed by the Technology Services Department.

Users are not prohibited from accessing their workstations or servers remotely unless those specific workstations or servers are behind a firewall.

Workstations and servers located behind a firewall can be accessed for administrative purposes by using a secure remote access solution.

Connections using Terminal Services, PC Anywhere or any other remote access software are not permitted through firewalls, including DMZ's. Exceptions to this rule must be reviewed and approved by the Technology Services Department.

5.0 Definitions

Communications Network – A system of communications equipment and communication links (by line, radio, satellite, etc.), which enables computers to be separated geographically, while still 'connected' to each other.

Computer System – One or more computers, with associated peripheral hardware, with one or more operating systems, running one or more operating systems, running one or more application programs, designed to provide a service to users.

Data / Information – In the area of Information Security, data is processed, formatted, and re-presented, so that it gains meaning and thereby becomes information. Information Security is concerned with the protection and safeguard of that information, which in its various forms can be identified as *Business Assets.*

DSL – Digital Subscriber Line, digital transmission over ordinary copper telephone lines.

Internet – A publicly accessible Wide Area Network that can be employed for communication between computers.

Network – A configuration of communications equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to each other. See also Communications Network.

Operating System – Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than processing work for users. Computers can operate without application software, but cannot run without an operating system.

Procedure – Detailed step-by-step actions to achieve a certain task.

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

Standard – Rules indicating how hardware and software should be implemented, used, and maintained. They ensure that technologies and applications are carried out in a uniform way across an organization.

SSL – Secure Sockets Layer, manages security of message transmissions over the Internet.

VPN – Virtual Private Network, using public telephone communications infrastructure to provide secure access to an organizations network.

6.0 Responsibilities

Technology Services:

- Development and maintenance of the Remote Access Policies, Guidelines and Procedures.
- Installation and maintenance of all equipment supporting Remote Access at the College.
- Performance and security monitoring for all steps of the remote-access process.
- Responding to problems reported to the Technology Services Help Desk in accordance with standard procedures and levels of service.
- Technology Services reserves the right to refuse any request involving Remote Access that may compromise the security of the College's networks.

User:

- Adherence to Policies, Procedures, Standards, and related guidelines established by the College and the State of Virginia including Policy Manual Section 1.61, "Telecommuting" of the Human Resource Policy Manual of the Virginia Department of Human Resource Management, effective 08/16/2002, revised on 09/10/05. The link to the cited HR policy is: www.dhrm.virginia.gov/hrpolicy/policy/telecommute1_61.pdf
- It is the responsibility of the user to ensure that unauthorized users are not granted access to the College's network through their remote connection.
- Implement the recommended security software, hardware settings, patches and protocols on personal equipment used to access the College's network via remote access technology. Personal machines used in this manner become a de-facto extension of the College's network.

- Follow all relevant College policies and procedures along with federal, state and local laws pertaining to the security of sensitive and confidential data when working with such data on the College's networks.
- Immediately reporting known misuse or abuse of the network or associate equipment to the Technology Services Help Desk.
- Any person found to have violated this guideline may be subject to corrective action.

7.0 Procedures

College units are responsible for requesting assistance with remote access implementations. Requests for such assistance will be made to and fulfilled by the Technology Services Department.

All computers connecting to the College's network via one of the remote access solutions listed in the Applicability section of this document shall use anti-virus software with the most up-to-date definitions available.

In addition, all computers connecting to the College's network via one the remote access solutions listed in the Applicability section of this document shall use the Microsoft Windows 2000 or Windows XP operating system. All critical security related software updates and service packs recommended by Microsoft shall be applied to the remote computer's operating system.

Remote access users will be automatically disconnected from the College's network after approximately 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep a connection open.

Dual or split tunneling is not permitted when using a VPN-based connection. Dual or split tunneling allows a remote computer to connect to both the Internet and a VPN connection simultaneously.

8.0 Sanctions

9.0 Interpretation

Authority for interpretation of this policy rests with the College president and vice president of financial administrative services.

10.0 Authority/Reference

Policy Manual Section 1.61, "Telecommuting" of the Human Resource Policy Manual of the Virginia Department of Human Resource Management, effective 08/16/2002, revised on 09/10/05. The link to the cited HR policy is: www.dhrm.virginia.gov/hrpolicy/policy/telecommute1_61.pdf .

Attachment A

Lord Fairfax Community College

Remote Network Access Request Form

Complete and sign the following:

___ Add New User ____ Update User

Name: ____
(Print) First Name Middle Initial Last Name

Office \ Division Name: __________________________________

Campus or Center: ____ Middletown ____Fauquier
____Middletown Courts ____ Luray-Page

Accounts requested (check only one):

___ **Terminal Services** – Access to the College's standard desktop applications and to the user's network drives via Microsoft Terminal Services. This access will require that the requestor install Cisco Systems VPN (Virtual Private Network) Client and enable and configure Microsoft Remote Desktop Connection on their remote computer.

___ **Direct Connection your Office Workstation** – This access will require that the requestor install Cisco Systems VPN (Virtual Private Network) Client and enable and configure Microsoft Remote Desktop Connection on their remote computer. In addition Technology Services will need to configure Microsoft's Remote Desktop Services on the requestor's office desktop computer.

Note: By singing below I acknowledge that I have reviewed and understand the College's Remote Network Access Policy.

Employee's Signature: ______________________ Date: ________

Immediate Supervisor's Signature: _______________ Date: _____

For Technology Services Use Only:

___ **Terminal Server Remote Access Account**

Created by: __________________________ **Date:**____________