NEW COLLEGE OF FLORIDA
REGULATIONS MANUAL

CHAPTER 4 - Academic Affairs

4-5007 Virtual Private Networking (VPN)

Virtual Private Networking (VPN) is a method of connecting users who are not physically on the College's campus with the New College network. Users can access and work with their files stored on campus servers from any remote location that provides Internet access via high-speed lines or modems.

(1) Definition. VPN allows users to access and manipulate files stored on campus servers from remote locations. This eliminates the need to travel with sensitive or confidential data or to save such data on a remote computer. Another important advantage of VPN is that valuable files such as drafts of books or articles can be stored and backed-up on campus servers and accessed at any time and place. The VPN creates a connection between a user's remote computer, for example a personal computer used at home or elsewhere, with a user's files stored on a campus server. Once connected, the computer screen, folders, and files are indistinguishable from those the user sees when using their on-campus computer. A user accesses VPN through a link on the New College website, using their network user ID and password.

(2) Users. Any current employee of the College may use the VPN service.

(3) Data Access. A user may access and manipulate any files that they have access to using their on-campus PC. When VPN is in use, users should not use their web browsers to access the World Wide Web.

(4) Security of Computers and Data

   (a) Remote, user-owned computers connected to the College's VPN service become an extension of the College's network and in turn provide access to that network. They are subject to the same rules and regulations that apply to College-owned computers, and especially those concerning data security. Remote user-owned computers must have the latest operating system or applications updates installed. These updates ensure that the latest security features are active. Current anti-virus software is required on any remote user-owned computer accessing the College's VPN. The antivirus software must be active with automatic updates and scheduling features turned on. Failure to update this software and ensure it is active will constitute a violation of the College's VPN policy and could subject the user to College discipline and personal liability. Because VPN allows off-campus users to access the College network and servers, it is particularly important that passwords must not be shared and that antivirus software must be installed.

   (b) Non-New College employees are not permitted to access this service. Confidential data stored on the College's network and accessed on user-owned or college-owned, remote computers through VPN should not be downloaded and stored on remote computers or external storage devices, including, but not limited to, USB thumb drives, disks, or hard drives. Examples of confidential data include social security numbers, home addresses, course evaluations of student work, and faculty promotion files. Confidential information is protected by state and federal laws, and violations of this policy could subject the user to civil and/or criminal prosecution.

(c) VPN users will be automatically disconnected from New College's network after sixty minutes of inactivity to help prevent unauthorized use. The user must then log-in again to reconnect to the network.

(d) More information regarding software, security patches and anti-virus software can be found at http://www.ncf.edu/it.

(5) Activation. To utilize VPN, place a Help Desk ticket to have remote access enabled on your PC. IT will change the necessary settings on your PC and check to ensure that the latest versions of the operating system and anti-virus software are installed and active. Once remote access is enabled on your on-campus PC you can access it from a remote PC by going to the Faculty & Staff page (http://www.ncf.edu/index/faculty-staff) on the NCF website and clicking on the NCF VPN link under Faculty/Staff Resources. Use the same user ID and password that you use to log on to your on-campus PC.

(6) Internet Access. VPN use from any remote location requires Internet access. The user is responsible for arranging for that access and its associated costs.

Authority: Article IX, Sec. 7, Fla. Constitution; Fla. Board of Governors Regulations 1.001 and 3.0075

History: Adopted 03-05-11; Revised 02-26-17 (technical amendment)