



Blue Mountain Community College *Administrative Procedure*

Procedure Title: Virtual Private Network
Procedure Number: 04-2011-0001
Board Policy Reference: IV.A.

Accountable Administrator: VP of Operations
Position responsible for updating: AVP, Information Technology
Original Date: 02-23-2011
Date Approved by Cabinet: 04-12-11
Authorizing Signature: *Signed original on file*
Dated: 4-12-11
Date Posted on Web: 11-1-13
Revised:
Reviewed: 10-13

1.0 Introduction

In an effort to provide essential security for the Blue Mountain Community College information technology network and its associated systems, routine off-campus access to many information technology resources is necessarily restricted and administratively controlled. There are, however, some faculty or staff members for whom off-campus access may facilitate the performance of their essential duties, e.g., information technology personnel who may remotely monitor and respond to information technology system malfunctions; maintenance personnel who may access security systems or HVAC-control systems from remote locations; or senior executives who may be off site but need to access information inside the firewall. To meet these needs, the College has established a Virtual Private Network (VPN) for users who have an appropriate need to access information technology systems that are not routinely available from off-campus networks. The vice president for operations evaluates the need for and authorizes such access; the associate vice president for information technology provides and administers access that has been duly authorized. It should be noted that VPN access is not intended to provide the equivalent of telecommuting or teleworking, i.e., VPN access is not intended to provide the capability to routinely work at home or outside the workplace instead of at the office or for the simple convenience of a faculty or staff member. VPN access brings its own set of vulnerabilities, so the authorization for its use will be specific and limited and not general in nature.

2.0 Purpose

The purpose of this procedure is to provide administrative guidelines for VPN connections to Blue Mountain Community College's internal network. Blue Mountain Community College's VPN server is designed to provide secure (encrypted) access to network resources on the Blue Mountain Community College network.

3.0 Definitions:

VPN Virtual Private Network: a virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network

Connection A single encrypted link between the BMCC network and a remote device.
DSL Digital Subscriber Link
User Personnel who are authorized to access Blue Mountain Community College network resources using a VPN connection

4.0 Guideline:

4.1 VPN gateways will be set up and managed by the Blue Mountain Community College Information Technology Department.

4.2 Only VPN client software that is approved by and/or distributed by the Office of Information Technology networking services may be used.

4.3 By using VPN technology with either personal or College equipment, users must understand that their machines are an extension of the Blue Mountain Community College network and, therefore, that they must comply with all Blue Mountain Community College procedures, including but not limited to the [Use of College Electronic Information Resources Procedure](#).

4.4 VPN provides secure access into the Blue Mountain Community College network, but VPN does not, by itself, provide Internet connectivity. Users are responsible for providing their own Internet service via dial-up, cable-modem, DSL, or other means to be able to use the Blue Mountain Community College VPN service. A static IP address from a user's Internet provider may or may not be required.

4.5 Currently, VPN software is available for Windows XP or newer operating systems. The Information Technology Department will provide instructions to approved users; users will be responsible for the installation of VPN software.

4.6 Users are responsible for ensuring that unauthorized persons are not allowed access to Blue Mountain Community College internal networks and resources. A user whose account is compromised by a phishing attempt or by any other means will be immediately removed from VPN access at least until the issue is resolved.

4.7 All computers, including personal computers or other devices, connected to Blue Mountain Community College internal networks via VPN must use current anti-virus software approved by the College and maintained current by the user. Failure to do so will be grounds for terminating VPN privileges.

4.8 VPN users will be automatically disconnected from the Blue Mountain Community College network after fifteen minutes of inactivity. The user must log on again to reconnect to the network. Pings or other artificial network processes shall not be used to keep the connection open; their use will be grounds for terminating VPN privileges.

4.9 Only one active VPN connection is allowed per user.

4.10 Using the VPN server to access Internet resources external to Blue Mountain Community College is not recommended.

4.11 Only prospective users approved by the Vice President of Operations will be authorized VPN access, and access will be limited to only those duties and activities authorized by the Vice President of Operations.

4.12 A prospective user may request VPN access via e-mail to his/her Department Head. The prospective user shall state in a comprehensive manner for what purpose VPN access would be granted and why the prospective user could not achieve the stated purpose from within the network (inside the firewall) during normal working hours. The Department Head shall forward his/her recommendation and rationale to his/her Vice President (or, for employees assigned to the President's staff, to the President),, who, in turn, shall forward his/her recommendation and rationale to the Vice President for Operations. The Vice President for Operations shall decide the matter and notify all appropriate parties of the decision. The Associate Vice President for Information Technology shall create and administer access for approved requests.

4.13 A VPN user who knowingly or unknowingly compromises the integrity of the Blue Mountain Community College network through the deliberate or unintentional misuse of his/her VPN access shall have that access terminated under the provisions of this procedure and, in addition, may be subject to other actions under such other policies or procedures that may be applicable to the circumstances.