POLICY TITLE: **VPN Policy**

POLICY #: **IT - 5**

DATE DRAFTED: **September 10, 2005**

APPROVED DATE: **October 10, 2005**

REVISION DATE:

VPN Policy

1.0 Introduction

In an effort to increase the security of Trinity Valley's information technology systems, off campus access to many information technology resources has been limited. Trinity Valley offers Virtual Private Network (VPN) access for administration/faculty/staff who need access to information technology systems that are not available to users from off-campus networks. Exceptions to the approved list of users will be considered on a case by case basis by the Dean of Information Technology Services.

2.0 Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to Trinity Valley Community College's internal network. TVCC's VPN server is designed to provide secure/encrypted access to network resources on the TVCC Network. Using the VPN server to access Internet resources external to the TVCC network is not recommended.

3.0 Policy

3.1 VPN gateways will be set up and managed only by Trinity Valley Community College Information Technology Services.

3.2 Approved users can request a CD containing the VPN client and installation instructions at the ITS help desk. For additional information about this CD you can email helpdesk@tvcc.edu.

3.3 Only VPN client software that is approved by and/or distributed by ITS networking services may be used to connect to the TVCC VPN server.

3.4 By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of TVCC's network, and as such must comply with Trinity Valley Community College's Information Technology Policies.

3.6 VPN provides secure access into the TVCC Network. 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 TVCC's VPN service.

3.7 Currently VPN software is available for Windows 2000/XP. Approved users are responsible for the installation of the VPN software.

3.8 It is the responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to Trinity Valley Community College internal networks.

3.9 Trinity Valley Community College has configured the VPN service to not allow the bridging of networks (split tunneling). As a result, when connected to VPN, all network traffic from the user's computer will travel through the Trinity Valley Community College network which will not allow

communication back to a device on the private network other then the computer making the original connection.

3.10 All computers, including personal computers, connected to Trinity Valley Community College's internal networks via VPN or any other technology must use the most up-to-date anti-virus software approved by TVCC IT Services.

3.11 VPN users will be automatically disconnected from Trinity Valley Community College's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes should not be used to keep the connection open.

3.12 Only one active VPN connection is allowed per user and the VPN concentrator is limited to a total connection time of 8 hours per user in one session.

4.0 Enforcement

Any user found to have violated this policy may be subject to loss of certain privileges or services, including but not necessarily limited to loss of VPN services.