

POLICY TITLE: Network Usage Policy
POLICY #: IT - 9
DATE DRAFTED: November 03, 2005
APPROVED DATE: February 03, 2006
REVISION DATE:

1.0 Introduction

The network is to be used in accordance with the mission of Trinity Valley Community College as a tool to enhance education and is not available for unrestricted use for other purposes. These policies are a supplement to the TVCC Acceptable Usage Policy and are subject to change.

2.0 Purpose

This policy is to ensure that TVCC network resources are used for the mission of Trinity Valley Community College.

3.0 Policies

- 3.1** Unauthorized networking equipment (such as routers, hub, and wireless access points, etc.) is prohibited from use on the network. Network services and wiring may not be modified or extended beyond their intended use. This policy applies to all TVCC infrastructure and services. Any unauthorized equipment such as routers, hub, and wireless access points, etc. found connected to the TVCC network infrastructure will be confiscated.
- 3.2** Personal computers and/or laptops may not be directly connected via a patch cable to the TVCC network infrastructure unless specific authorization is granted by the Dean of Information Technology Services. Any personal computer or laptop connected directly to the TVCC network infrastructure via a patch cable will be confiscated.
- 3.3** Users may not manually assign an IP address to any network device. Doing so may disrupt connectivity for other users on the TVCC Network. If a static IP address is needed you must contact IT Services for assistance. All static IP address will be assigned by IT Services The decision as to whether a static address is needed will be at the sole discretion of the Dean of Information Technology Services.
- 3.4** Users of the TVCC network may not provide access to resources on the local network to anyone outside of the college community for any purpose unless accomplished by means approved by the Dean of Information Technology Services.
- 3.5** All computers attached to the TVCC network infrastructure will be given computer names assigned by Information Technology Services. Computer names, computer descriptions, and messages broadcast across the network should not be defamatory, lewd, or obscene.
- 3.6** Network users are responsible for any network activity linked to their CardinalIDs. CardinalID passwords must be secure, and should not be shared with anyone (including family, work-study students, friends, and administrative assistants). Users who believe that another person is using their account should notify the Information Technology Services helpdesk immediately and change their password.
- 3.7** For security reasons, TVCC requires users to log on to access the campus networks and the Internet. Users are prohibited from attempting to circumvent the authentication

systems. In addition, users should not attempt to hide their identity or impersonate another's identity while on the TVCC network.

- 3.8** Users are responsible for security and privacy precautions to protect against computer viruses and other computer attacks which may result in loss of data, unintentional release of personal information, or negative impact on the college's technology services. Failure to take these prudent steps could result in the offending computer or account being removed from the network.
- 3.9** No shared resources may be connected to the TVCC network infrastructure without permission from Dean of Information Technology Services. These resources include but are not limited to servers, hubs, switches, wireless access points, printers, copiers, or IPTV cameras. Permission to connect a shared device must be submitted to the IT Services Help Desk at helpdesk@tvcc.edu.
- 3.10** All shared resources including servers, files, printers, wireless and other workstation computers must be protected with a secure password. Any sharing of resources without a password must be authorized by the Dean of Information Technology Services.
- 3.11** Federal law prohibits the transmission (sharing) of copyrighted materials without express written permission from the copyright holder. Copyrighted works (including but not limited to original writings, software, movies and music) may not be shared on the local network without written permission of the copyright holder.
- 3.12** Trinity Valley Community College reserves the right to restrict access to any service detrimental to the TVCC IT resources or a service that is not in keeping with the mission statement of the college. Attempts to bypass these restrictions will be considered a violation of this policy.
- 3.13** Trinity Valley Community College does not allow network users to run unauthorized SMTP, DHCP, or directory services on any networks.
- 3.14** Audio, video and game servers are not allowed on the TVCC network.
- 3.15** Defective, malfunctioning, compromised or misconfigured equipment on the network will be disabled without prior notification.
- 3.16** Unauthorized registration of a domain to a TVCC IP address is prohibited. This includes but is not limited to direct DNS resolution and DNS aliasing.
- 3.17** Unauthorized hardware and/or software used to detect and/or exploit network vulnerabilities are forbidden on Trinity Valley Community College networks.
- 3.18** It is the policy of TVCC Information Technology Services to not block any legitimate traffic. IT Services does reserve the right to use packet shaping to ensure that mission critical applications of the college are not compromised or degraded.
- 3.19** IT Services does not block any form of traffic to any website. IT Services does however shape the total bandwidth of TVCC's network to ensure that business & academic services have priority over recreational traffic.
- 3.20** Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited regardless of intent.
- 3.21** Student violation of these policies will result in loss of service. Violators may be forwarded to the Vice President for Student Services for further action.
- 3.22** Faculty or staff violation of these policies will result in a report being filed with the appropriate department head and possible disciplinary action.