Network Access Policy

Purpose and Scope

- The purpose of this policy is to define
  - The types of network connectivity that Information Technology (IT) provides users
  - Standards for connecting to the Wofford College campus network from any host, including all remote connections.
  - Criteria for gaining access to wireless data communications on the campus network.
  - Guidelines for Remote Access IPSec Virtual Private Network (VPN) connections to the campus network.
  - Guidelines for Remote Access Dial-In connections to the Wofford College campus network.
  - Activities that will potentially result in the loss of network access for a user or computer.
- This policy applies to anyone who accesses the Wofford campus network, including users of dial-in, wireless, VPN and other forms of remote access.
- This policy applies to all devices, both Wofford-owned and personal, which are used to access the Wofford campus network.
- The remote access section of this policy applies to, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, and cable modems
- The wireless access section of this policy applies to all wireless communication devices connected to the campus network.
  - This includes any form of wireless communication device capable of transmitting packet data.
  - It does not apply to wireless devices and/or networks without any connectivity to the campus network.
- The VPN access section of this policy applies to implementations of VPNs that are directed through an IPSec Concentrator.

Policy: Network Connectivity

- Wofford will provide the following types of network connectivity for users with accounts:
  - Direct wired connectivity for on-campus computers,
  - Wireless connectivity for on-campus computers,
  - Internet Service Provider access for remote connections to webmail and Banner Web
  - Dial-up modem access for Internet connections
  - In some cases, direct VPN access to the campus network through a remote connection.
- Limited network access for guests of the college will be furnished over an unsecured wireless network and on public computers located in computer labs and in kiosks.
  - All general policies contained within the current *Policy on the Responsible and Ethical Use of Wofford College Technology Resources* apply to guests.

    - The wireless Guest Network, which is meant for guests of the college, is not equivalent to the wired or wireless network used by Wofford students, faculty and staff.
        - Wofford services will not be available on the Guest Network – webmail and webs.wofford.edu, for example.
        - The Guest Network has limited bandwidth
        - There are few security measures in place on the Guest Network. Guests should have no expectation of privacy when they use this network.
    - The primary purpose of Wofford's network is to serve members of the campus community – Wofford students, faculty, and staff.
        - Guests are welcome to use the college network as long as their activities do not interfere with those of the campus community.
        - If guests' activities are interfering with those of the campus community, IT will require the guests to cease using the network.
- Computers connected to the campus network by any means can do so only to provide the user with access to existing information or to communicate new information via email, the web, etc. Users are not permitted use of devices to provide unauthorized services or act as gateways to provide alternative means of access to Wofford services.

Policy: Remote Access

- All general policies contained within the current *Policy on the Responsible and Ethical Use of Wofford College Technology Resources* apply to users of any kind of remote access, including, but not limited to, dial-in, wireless, and VPN.
- Remote access will be strictly controlled by the College's VPN and Remote Access gateways.
- In the absence of IT approval, the only acceptable forms of remote access are VPN, dial-in, and wireless. Organizations or individuals who wish to implement other forms of remote access to the College network must obtain prior approval from IT.
- All hosts that are connected to the campus network by remote access technologies must use the most up-to-date anti-virus software and operating system patches available; otherwise they will not be allowed to connect.
- Hosts that are remotely connected to the campus network must not be simultaneously connected to any other network, with the exception of personal networks that are under the complete control of the user.

Policy: Wireless Network Access

- To comply with this policy, wireless implementations must:
    - Maintain a hardware address, such as a MAC address, that can be registered and tracked.
    - Provide either
        - User authentication against the Wofford College Active Directory; or
        - Guest access on the College's Guest Network
    - Allow network access via a method that ensures privacy, authentication, and integrity of wireless communications, such as Protected Extensible Authentication Protocol in combination with dynamic Wired Equivalency Protocol encryption.

- Only IT is authorized to attach wireless access points (APs) to the campus network.
- Under no circumstances may non-IT owned APs be attached to open network ports anywhere on campus.

Policy: Virtual Private Network Access

- Only VPN gateways set up by IT are allowed on the campus network.
- Only IT-issued VPN client software may be used to access the campus network.
- VPN use is to be controlled using a combination of a one-time group password such as a shared key with a strong passphrase and user authentication against the Wofford College Active Directory
- It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed VPN access to the campus network. At no time should any Wofford College employee or agent provide their VPN client software or a VPN enabled computer to anyone.

Policy: Dial-In Access

- Only dial-in access set up by IT is allowed on the campus network
- The use of dial-in accounts will be monitored. If a retiree's dial-in account is not used for a period six months the account will be disabled.
- It is the responsibility of authorized dial-in users to ensure that their dial-in connection is not used by an unauthorized user.

Enforcement

- A user who is in violation of any policy within the current *Policy on the Responsible and Ethical Use of Wofford College Technology Resources* will be subject to the penalties described in that document.
- A user who is in violation of the Network Access Policy may be subject to disciplinary action by their Administrative unit or by the College. This may include revocation of certain network access privileges, such as VPN access.
- A computer determined to be infected or security-compromised in a way that is a threat to the network will have its network access revoked.
    - This includes Wofford-owned computers on which security measures, such as antivirus software, have been by-passed or disabled.
    - In extreme and widespread cases of infection, network access may be revoked for a significant portion of the college network, such as the Residence Hall network.
    - Network access will remain revoked until IT has verified that infected or compromised computers have been restored to health and updated virus protection has been installed.
- IT will monitor the local wireless network for unauthorized APs and other unauthorized wireless network devices that pose security risks.
    - A first-time violation will result in the wired network port associated with an unauthorized device being immediately disabled without notice. The unauthorized wireless network's hardware's MAC address also will be blocked at the network level. An attempt will be made to inform the owner of the unauthorized device of his or her violation.

    - Subsequent violations may result in more serious measures including the extended loss of access to network services.

Responsibilities

• Active Directory domain accounts	Ron Wood, 597-4273 Matt Fisher, 597-4274
• Network connectivity	Bart Casey, 597-4295 Brian Rawlinson, 597-4547
• VPN, wireless, and dial-in access	Bart Casey, 597-4295 Brian Rawlinson, 597-
• Kiosk computers	Help Center, 597-4357
• Wireless setup	Help Center, 597-4357