Computer Management Policy

Purpose and Scope

- This policy has four purposes:
  - To describe the Information Technology (IT) computer resource management system, which provides for centralized management of computers, including standardized configurations, security, authentication, and shared resources.
  - To describe the rights and responsibilities of Wofford staff who use computers managed by IT.
  - To describe the responsibilities of Wofford IT staff who manage computers.
  - To ensure that users of multi-use classroom computers will always find these computers in the same default configuration when they begin their class.
- This policy applies to all desktop, laptop/notebook, and tablet PCs; Macintosh computers; other computers owned by Wofford College and managed by IT; and to all users of these computers

General Policy: Managed Computers

- All managed computers will be furnished with the same basic software, some of which is listed below. The software versions will change over time.
  - Windows software: Microsoft Windows, Microsoft Office Professional, Symantec Antivirus, Internet Explorer, and Adobe Acrobat Reader
  - Macintosh software: Mac OS, Microsoft Office Professional, Symantec Antivirus, Internet Explorer, and Adobe Acrobat Reader
  - All managed computers will connect to an Active Directory domain for user and group level authentication.
- All managed computers will be furnished with standard security precautions, such as antivirus software and password-protected screensavers.
  - A central virus server controls the installation of virus definitions an all managed computers. Symantec Antivirus Corporate Edition periodically runs an updater service every two hours to ensure that the most up-to-date virus definitions are installed.
  - If a computer has not been used for 90 minutes, a password-protected screensaver locks the computer and requires the user to enter his or her username and password to continue. This can help prevent unauthorized persons from using a computer and having access to our network while the computer's rightful user is absent.
- All managed Windows PCs will have patch management controlled by a Windows Update and Group Policy.
  - Each machine is scheduled to check for updates once a day
  - If any critical updates exist, then the patch is installed and users are prompted to reboot their machine, if a reboot is required.
  - Non-critical patches are applied through the Microsoft Windows update service.

- All managed computers will be capable of remote management over the campus network.
    - IT will remotely install new or upgraded applications on managed machines as needed.
    - With a user's permission, IT staff may connect to the user's computer, view the screen, and control the mouse and keyboard. This will facilitate troubleshooting of problems on the user's machine.
    - IT staff also may remotely manage a user's computer if approved by the individual's supervisor and the Vice President of Technology.

Policy: Computers Furnished for Users' Personal Use

- Users will be given limited administrative rights on their computers so that they can install nonstandard software when necessary.
    - Users will not install or use software that interferes or conflicts with the operation of IT's computer resource management system or other required software such as virus protection.
        - This includes the installation of personal firewalls, non-approved virus protection, add-on screensavers that are not part of the computer's operating system, and others.
    - The installation of peer-to-peer (P2P) file-sharing software is expressly forbidden.
    - IT will not be responsible for supporting nonstandard software
    - In the event that a computer system fails, IT technical support will be limited to the recovery of the system by reinstallation of the basic software (OS and standard applications) that was installed on the computer when it was originally placed in service. Nonstandard applications installed by the user will not be replaced.
- Although IT manages computers, users will assume the responsibility for managing the application software (e.g., Microsoft Word, Excel, and PowerPoint) that they use.
    - Managed computers will be furnished with application software in the default configuration furnished by the manufacturer.
    - Users may change settings on application software to suit their individual preferences. They will be responsible for any and all changes in application software configurations that they make, however.
    - In the case of improperly configured application software, IT technical support will be limited to the recovery of the system by reinstalling the basic software that was on the computer when it was originally placed in service. In extreme cases, this may require wiping the hard disk of the computer, in which case all data may be lost.
- Users will not attempt to alter computer settings that might compromise the security or performance of a managed computer system.
    - This includes, but is not limited to, network configurations, Windows registry, antivirus software settings, screen-saver settings, and remote management settings.
    - With authorization from the Vice President of Technology and the user's supervisor, IT staff may monitor a user's activity for attempts to change settings or circumvent computer security.

- Users should not rely on the storage on their computers
    - They should back up important files, either on their network storage or on removable media, such as a USB flash drive or an external hard drive.
    - IT will not be responsible for the recovery of data in the event of a computer system's failure.

Policy: Multi-Use Lab or Classroom Computers

- This section of the policy applies only to computers that are used by several faculty members, generally in a classroom situation.
    - It applies, for example, to any computer located in shared classrooms in the following buildings:
        - Daniel Building
        - Main Building
        - Olin Building
        - Roger Milliken Science Center
    - It does not apply to research laboratory computers that are used by only one or two faculty members, such as computers located in one of the RMSC Science Department research laboratories.
    - It does not apply to computers located in rooms maintained by one department for use by their students, such as the Foreign Language multimedia lab or the Science Department computer labs.
- Administrator rights on multi-use classroom computers will be limited to Help Center staff, who will be responsible for managing all application software on these computers
    - Faculty members who need non-standard applications loaded on these computers must bring an installation CD to the Help Center at least two weeks before they need the application on the machine.
        - Along with the installation CD, we must have evidence of licensing to install the software on an individual computer.
    - The Help Center staff will make every effort to install application software that has been requested for multi-use classroom computers less than two weeks in advance. We cannot guarantee that installation by the requested date will be possible, however.
- As part of this program, Help Center staff members assume the following responsibilities
    - Around July 15 and December 1 of each year, we will remind faculty about the two-week software installation deadline for the beginning of the Fall and Winter terms, respectively.
    - We will check classrooms proactively before the beginning of each semester, looking for potential situations in which a faculty member may not recognize that he or she needs application software installed.
    - In case of a last-minute classroom change, installing needed application software in a classroom to which a professor has been moved will be highest priority for Help Center staff, taking precedence over virtually every other task.

Policy: Academic Computer Laboratory Computers

- This section of the policy applies only to computers located in Olin 207 or the Great Oaks Hall public computer lab
- Faculty members who need non-standard applications loaded on the lab computer image must bring an installation CD to the Help Center at least six weeks before they need the application on the machine.
- Faculty members who need non-standard applications loaded on five or fewer lab computers must bring an installation CD to the Help Center at least two weeks before they need the application on the machine.
- In either case, along with the installation CD, we must have evidence of licensing to install the software on an individual computer.

Enforcement

- IT will follow the procedure below in the event that a user has compromised security precautions that have been installed on his or her machine.
    - IT staff will examine the machine to confirm that there actually is a security problem
    - In the case there is a problem, IT staff will inform users of the importance of security on the machine and advise them of ways they can avoid compromising the security feature again.
    - IT staff also may install computer security software to monitor for and/or prevent users from making inappropriate changes to their computers.
    - With authorization from the Vice President of Technology and the user's supervisor, IT staff may monitor a user's activity for attempts to change settings or circumvent computer security.
    - In the cases of repeated situations in which a user compromises security precautions on a Wofford-owned computer, IT will notify the user's supervisor for appropriate disciplinary action.
    - If the behavior persists, IT will remove the user's machine.
- IT will follow the following procedure in the event that a user has improperly configured application software to the extent that it is unusable.
    - IT staff will reinstall the basic software (OS and standard applications) that was on the computer when it was originally placed in service
    - In the case of repeated incidences of improperly configured application software, IT will no longer furnish technical support to that user for this software.

Responsibilities

• Furnishing computers	Help Center, 597-4357 Chris Myers, 597-4279
• Antivirus and patch management	Matt Fisher, 597-4274
• Computer management and troubleshooting	Help Center, 597-4357 Martin Aigner Todd Camp Nathaniel Colvin James Dawson Scott Sperka
• Authorizing monitoring	David Whisnant, 597-4294