INSTITUTIONAL DIRECTIVE 2-9

July 24, 2006

Title: Institutional Security of Personal Computers and Internet Resources

I. Purpose

The purpose of this directive is to set forth policy relating to the use of personal computers and the Internet in a safe and secure manner.

II. Policy

It is the policy of Piedmont Technical College to provide a secure environment for the processing of data on personal computers and to ensure that data loaded onto personal computers or downloaded from the Internet is free of viruses and other security hazards.

III. Philosophy

Personal computers provide rich surroundings for those intent upon computer crime. PC's are vulnerable to a variety of situations where data may be lost and hardware destroyed by programs and procedures know as "viruses" which infect the system and cause problems in countless ways. As systems are connected to various networks the threat of contamination increases exponentially. In the absence of protection from these dangers, lost work, lost data and system downtime are the only probable results. In addition, usually, more than one computer is affected. In a networked system, it is quite possible for all the PC's on one Local Area Network (LAN) to suffer from the same symptoms.

As systems are connected to the World Wide Web (WWW) large amounts of new data and many new programs are available to the PC user. By just "clicking" a mouse, the PC user can download whole disks full of data and applications. Unfortunately, some of this information and some of the programs contain viruses and the infection is complete as soon as the data starts to download. Without some means of protection, a minute's work on the Web will result in hundreds of hours of downtime and frustration. The answer to this situation is the use of a Firewall which filters all incoming information and detects unreliable data. The Firewall also protects the LAN from nefarious users who penetrate the system and either download dangerous information, or take information from the PC. This system of security provides protection from outsiders who are intent on computer crime.

Other security problems exist from data entering individual PC's via diskettes. A favorite method for downloading a virus is to place the viral code on the header record of a diskette, memory key or other storage device, which automatically installs the virus when the media is read for the first time.

Office of Responsibility: President

The answer to this manifestation is an interactive virus protection program which interprets every computer transaction and tests it for viral infection. The third method for access is an unprotected PC left unattended. An unprotected PC is one which does not have a password scheme in place. In such a case, the miscreant simply accesses a PC that is left unprotected. It makes no difference that the PC is turned off; unless the system is locked by a password, it is vulnerable. Protection for the PC environment then comes from a combination of a Firewall, virus protection and pass wording. With these three measures in place, probability of loss of data or hardware is significantly reduced.

Another serious problem with computers is the possibility of compromise of protected data such as student personal information. If proper care is not exercised, unauthorized personnel are provided with opportunities to read and capture protected information by looking at protected information on screens or by accessing protected data via networks or by accessing unprotected computer systems.

IV. Procedures

A. All personal computers on campus and in off-campus locations will have an interactive virus protection program installed and running at all times. This program will be updated by the appropriate office as soon as new releases of the program are made available.

B. All administrative personal computers on campus and in off-campus locations will have a password activated screen saver configured for a minimum timeout period of fifteen minutes. This will be activated by Information Services personnel via Active Directory rules. In the case of open labs, each PC will have a "disk-lock" mechanism and will be unlocked by the lab assistant each time a student requests access to a machine. Students will not have access to the passwords.

C. A Firewall system will be in place to provide protection from outside intruders. This Firewall will be located in a physically secure location.

D. Protected information will be safeguarded by:

1. Proper security within applications to ensure that only those authorized to see protected data may do so. This will be accomplished by limiting screen and element access to those using the software. Each functional area will determine who may view, update and delete the data associated with that office and inform Information Services who will implement the security measures.
2. Where information is displayed on video displays, care will be taken to ensure that unauthorized viewing is not possible by positioning displays carefully, or by utilizing optical technology in the form of polarized filters as necessary.
3. When protected information is in printed form, cover sheets, locked filing cabinets, vaults and shredding of unneeded documents will protect them from unauthorized viewing.
4. All personnel having access to protected information will be trained in safeguarding and otherwise protecting the data.

V. Responsibilities

A. Responsibility for ensuring that passwords and virus protection schemes are available and in use on all PC's will be the joint responsibility of Information Services and Instructional Technology staffs.
B. Responsibility for the Firewall system will reside with the Director of Information Services and his designated representatives.
C. Information Services will be responsible for all administrative machines and Instructional Technology will be responsible for those PC's used for instruction. The Information Services and Instructional Technology offices will have responsibility for auditing and enforcing the protection of sensitive data items in their respective areas.

Original on File **7/24/06**
Approved for Publication **Date**