**PHYSICAL PLANT**
**OPERATING POLICY AND PROCEDURE**

**PP/OP 01.04: Network/Personal Computers**

**DATE:** April 7, 2011

## PURPOSE

This PP/OP will provide basic information and guidance to Physical Plant personnel so that they may adequately safeguard the computing environment, ensure the integrity of the data generated and maintain the confidentiality of our information, and protect the investment the Physical Plant has made in this technology.

## REVIEW

This Physical Plant Operating Policy/Procedure (PP/OP) will be reviewed in March of each year by the manager for physical plant information systems and recommendations for revision forwarded to the managing director for physical plant.

## POLICY AND PROCEDURE

1. Introduction

   University objectives and external requirements mandate that personal computers and related peripherals be properly managed. This policy contains rules and working guidelines to be applied to the use of this technology at Physical Plant.

   Physical Plant's intention is to provide each employee reasonable access to the technology required to fulfill the responsibility of their position. The objective of this policy is to adequately safeguard the computing environment and to ensure the appropriate integrity of the data generated, maintain information confidentiality, and reasonably protect the significant investment made in this technology.

   It is the responsibility of individual users to adhere to the guidelines set forth in this policy and violations will be subject to the same disciplinary actions that accompany infractions of other Physical Plant policies. All personal computers and software are the sole property of the Physical Plant.

2. Information Systems Development Priority (ISDP) Committee

   Representatives from each of Physical Plant's functional groups will meet and establish priorities for software development and approve new PC software packages. The Managing Director for the Physical Plant will chair the committee, which will meet on a schedule he deems appropriate.

3. Network Specialist

The responsibility for day-to-day operations of PCs, networks, and peripherals will be with the Physical Plant's Information Systems section, specifically the Network Specialist and/or a designated backup.

The Network Specialist will be responsible for:

a. Installing all PC software packages approved by the Physical Plant,

b. Monitoring and maintaining all PCs in good working order,

c. Correcting all network and PC problems,

d. Assisting user sections with individual software and hardware problems and questions, and

e. Maintaining an accurate and up-to-date hardware and software inventory.

4. Personal Computer Hardware

a. Hardware Standards

All hardware acquired, including PCs and peripherals, will be of reputable industry standard to allow for a continuity of products, availability of maintenance, and an adequate supply of replacement parts.Compatibility with other Physical Plant technology will be a prime consideration. Requests for non-standard products will not be approved if a standard product will provide the required functions.

b. Hardware Re-deployment

New equipment will not be purchased if existing equipment is available to meet requirements. Deployment or re-deployment of technology will be based on sound justification and approved equipment configurations. Equipment will be matched to the functional requirements of the job being performed.

c. Hardware Inventory

The Network Specialist will maintain an accurate inventory of all PC and peripheral hardware. The inventory listing will contain the following:

(1) Specific physical location,

(2) Brand name, model, description, and serial number, and

(3) Fixed Asset number assigned by TTU Asset Management.

The Network Specialist will conduct an inventory of all PC hardware as required by University policy.

d. Hardware Maintenance

All hardware deemed critical to the Physical Plant function will be kept under a maintenance contract with a reputable source that guarantees minimal interruptions due to hardware failure.

The Network Specialist should be notified immediately of any problem occurring with equipment. Problems should be reported to BM&C Work Control. The Network Specialist or designee will determine whether outside vendor service is required.

e. Personal Hardware

To limit the Physical Plant's risk of exposure to viruses or hardware conflicts that may harm the system, no employee's personally owned hardware may be used on any Physical Plant PC without the approval of the Network Specialist.

5. Personal Computer Software

a. Approved Software Listing

Any software used by Physical Plant will be obtained from a reputable dealer or agency to ensure a continued source of support, enhancements, and the software meets all legal guidelines.

The ISDP Committee will approve all PC software for the Physical Plant (except those deemed appropriate by the IS Manager for network management, maintenance, communications, operating systems, or utilities required for the installation of connected devices). The Network Specialist will maintain an Approved Software Listing (Attachment A). Additions or deletions to this listing can be authorized only by the IS Manager.

Only legally obtained software, purchased and used according to the manufacturer's license agreement, will be used.

The Internal Audit Department will use the Approved Software Listing as part of their routine examination of individual user departments.

b. Software Licensing

Each user is responsible for conforming to the terms and conditions associated with the license agreement for each software application package. Using or creating copies of Physical Plant-owned software is strictly prohibited. Violators of this policy will be subject to disciplinary action.

Pirating software is a felony. Anyone found guilty of copying software may face possible fines of as much as $250,000 and prison term of up to five years.

The Physical Plant complies with the Digital Millennium Copyright Act described at: www.ttu.edu/dmca.php

c. Standards

The IS Manager will evaluate requests for software purchases, giving prime consideration to product/version standardization.

d. Exceptions to Standards

For purposes of this policy, existing standalone versions/releases of approved software are "grandfathered."

Individual requests for version upgrades to standard Physical Plant-wide programs will be considered on a case-by-case basis. The IS Manager will evaluate these requests taking into consideration time savings, projected frequency of use, estimated cost of the upgrade, critical nature of the processing, and impact on existing software and hardware. Final approval rests with the ISDP committee.

Note: The Network Specialist will only support the "Physical Plant-wide" version of any software. The responsibility for supporting options and utilities offered in different versions will fall to the individual user or department.

Specific application software for individual user departments will be evaluated on a case-by-case basis. Wherever possible, compatibility with existing Physical Plant hardware and software will be of prime importance.

Installation of all software, software upgrades or (use of) a demonstration program is to be done only under the direction of the Network Specialist. Each software package should be loaded into its own subdirectory (using the default installation) for easy identification and organization.

e. Software Inventory

The Network Specialist will maintain a master software inventory. This inventory will include the following information:

(1) Software name and version,

(2) License number,

(3) Location, and

(4) Network or standalone.

A review of this software inventory will be completed as part of the annual hardware inventory to be conducted by the IS Manager.

The Network Specialist will remove any obsolete software packages or versions from the PCs. Any removed, licensed software that still meets the Physical Plant's software standards will be retained by the Network Specialist for possible redeployment to other users, if appropriate.

All original program media will be maintained under the control of the Network Specialist in a safe, secure area.

6. Computer Viruses

The Physical Plant has installed and maintains anti-virus software on all PC's. The anti-virus application will allow for automatic scanning of any incoming files transferred through a modem or through the Internet or imported with diskettes. Disabling **anti-virus scanning is prohibited!**

The following guidelines apply to Internet use at Texas Tech University Physical Plant:

a. Internet access is enabled on all Physical Plant PC's.

b. Anti-virus software **must** be running on any PC used to access the Internet.

c. Absolutely no freeware, shareware, or other programs are to be downloaded without approval of the IS Manager. This includes but is not limited to "Chat" programs, Instant Messaging (IM), and Internet applets (weather, music, screen savers, etc.).

d. Items must be downloaded legally. If upgrades to products are downloaded, the Physical Plant must be legally licensed to do so.

e. Use of the Internet is governed by TTU Operating Policy and state law. Applicable law and policy can be found at: www.itts.ttu.edu/documentation/laws/

7. Security

All users of Physical Plant PC's are responsible for the PC's physical safety as well as the safety of the PC software and the information it processes. Employees are responsible for immediately reporting any violations, abuses, or other security weaknesses to their supervisors.

a. Hardware Security

It is the responsibility of the individual users to bring to their supervisor's immediate attention any suspected tampering with their PC hardware.

Moving or transferring any PC hardware will be done only under the supervision of the Network Specialist or Help Desk staff member.

No vendor will remove any PC hardware from Physical Plant premises without first giving a written receipt to the Network Specialist.

b. Local Area Network Security

Security over Physical Plant local area networks will be evaluated by the IS Manager. The level of such security will be commensurate with the vulnerability and importance of the application being accessed and the sensitivity of the data being processed.

Passwords will be the security control over software access when appropriate. Multiple layers of passwords will be used to minimize accessibility by unauthorized personnel.

c. Sign-On/Sign-Off Procedures

Employees should sign-off PCs and the network when away from their desk for an extended period of time such as lunch. Signing off at the end of the work period is **mandatory.**

d. Password Protection

Passwords are the key to unlocking important, and often times, confidential computer information. It is critical to properly protect passwords and make them hard for someone to guess. The University maintains a global network password system (eRaider). The Physical Plant is responsible for protecting several local applications (4Site, HRMS, etc.) with unique passwords.

Passwords will be a minimum of five characters. The password should contain at least one numeric character. The password should not, however, be so elaborate that it is difficult to remember.

Passwords should not be associated with anything personal including names or phone numbers. Passwords should not be shared with others or written down so others may gain access to them.

Passwords should be changed immediately if a user suspects that someone has gained knowledge of a password. The individual user is responsible for any unauthorized access to the system caused by sharing or otherwise making passwords available.

e. Networks

The University network is controlled by TTU.EDU through the use of the eRaider account management system. The eRaider system requirements are supported and maintained by the University as outlined at: http://www.depts.ttu.edu/itts/accounts/

f. Information Security

Information contained in Physical Plant's computing environment is considered a university asset. The wide use of PC generated information has created opportunities for abuse and unauthorized use of these assets.

Accidental disclosure of customer, employee, and/or university information could have a significant detrimental impact on the Physical Plant and/or the university.

Discarding PC information (on paper or magnetic media) containing sensitive or confidential information should be done with extreme care and follow other Physical Plant policies and procedures for this type of data.

The Physical Plant complies with the Texas Tech University privacy policy as outlined at: www.ttu.edu/privpolicy.php

g. Other Security Items

Users should sign-off the network if their PC will be unattended. **All individual users are accountable for all activity and access that occurs under their logon passwords.** Additionally, users should exit any software application that is not being actively used. The Physical Plant purchases a limited number of licenses of certain software applications. When users access one of these programs one of the licenses is considered "used" even though the user may not actually be performing functions within the program. This action may restrict other users from gaining access to the program when needed.

8. Personal Use

The PC equipment and software are the sole property of Physical Plant. It is recognized however, that the Physical Plant encourages community involvement and continuing education for its employees. Personal use of Physical Plant-owned hardware and software will be allowed providing some guidelines and limits are applied.

Personal use may be allowed if, in the judgment of individual section managers, it is not excessive, does not interfere with the normal conduct of business, does not involve a for-profit personal business activity, or have the potential to embarrass the Physical Plant or Texas Tech University.

All other rules and regulations set forth in this policy also apply to personal use. In addition, use of personal software on Physical Plant PCs is prohibited unless specifically approved by the IS Manager.

RESPONSIBILITIES

| Position | Section | Month |
|---|---|---|
| Manager for Physical Plant Information Systems | REVIEW | March (Each Year) |

Approved: _____
Reviewer

Approved: _____
Managing Director for Physical Plant