INTRODUCTION

Information Technology services including, staff, workstations, peripherals and network infrastructures are an integral part of The Division of Student Affairs at The Pennsylvania State University’s University Park campus. Student Affairs has and continues to provide substantial investments in resources to provide these services to our staff. Protect your privacy and the division’s physical and intellectual property by following the policies and procedures outlined in this document.

PURPOSE

The purpose of the policies and directives that follows have been established in order to:

- Protect the Division’s investment.
- Secure the electronic information (data) within our systems.
- Reduce the risk to the University and the Division from internal and external sources.
- Provide guidelines to Student Affairs staff when using our resources.
- Protect the Penn State name and the integrity of Student Affairs.

This policy provides guidelines for the use of Student Affairs computer equipment and network services. It emphasizes the importance of individual responsibility in maintaining a secure computing environment. Student Affairs staff who requests an access account must review this policy prior to being assigned an account. The Student Affairs networks, workstations, file / print services, e-mail services and other network applications are to be used for University business purposes, with exceptions as provided in this and other University policies.

POLICY / PROCEDURE:

POLICY ABUSE

Violations of any policy may result in disciplinary action in accordance with University policy and may result in:

1. Restriction or termination of a system user's access to Student Affairs Computer and Network Resources, including the summary suspension of such access, and/or rights pending further disciplinary and/or judicial action;

2. The initiation of legal action by the University and/or respective federal, state or local law enforcement officials, including but not limited to, criminal prosecution under appropriate federal, state or local laws;

3. The requirement of the violator to provide restitution for any improper use of service.
Network and Workstation Acceptable Use Policy

4. Disciplinary sanctions, which may include dismissal or expulsion for students, or termination for employees.

1 Student Affairs staff includes all permanent and or temporary staff including work-study students who are assigned a network access account. University Health Services staff must refer to Appendix A for the applicable Policy on Workstation Security and Privacy and Security Agreement. Student Affairs Information Technology has the authority and responsibility for the entire Division including University Health Services (Student Health Services).

POLICIES AND GUIDELINES FOR STUDENT AFFAIRS STAFF

1. INTERNET AND E-MAIL USE:
   A. Access to the Internet is provided to staff for the benefit of Student Affairs conducting the business of Student Affairs.
   B. The Internet is filled with risks and inappropriate material. To support a safe, responsible and productive environment, the use of the Internet and e-mail is to be used for Student Affairs business only.

2. PASSWORDS
   A. You will be issued a unique network (personal) access account for the Student Affairs domain. You are responsible for appropriately securing your password. You may not share your password and may not login to the network using another person’s unique account. The Division’s limited group accounts (member with several others) have been specifically authorized by the Vice President of Student Affairs and approved by the Directors of Student Affairs Information Technology and ITS Security Operations and Services at Penn State. If you are assigned a group user account you may not share that account password with unauthorized persons.

   B. PASSWORD SECURITY

   • Your network account password is valid for a period of 90 days. Two weeks prior to the expiration of your password, you will receive a message advising you to change your password. It is suggested that you change your password as soon as possible after you receive that message. When your network account password expires, you will receive a message indicating that your password has expired. You will then be given the opportunity to set a new password. The system permits you just five tries to set a new password. So carefully type and re-type your new password. If for some reason you are unable to reset your password, you can contact our help desk for assistance at 865-7210.
   • To reduce the probability that your password will be compromised, it must contain between 8 and 14 characters. Valid Student Affairs passwords must also be comprised of a combination of letters and numbers and must contain at least one special character (a symbol, punctuation mark, or upper and lower case characters).
   • Example: The-qu1ck-f0X
3. MEMORIZING PASSWORDS

- Please do not write down and store your passwords in your office. Passwords are an important procedural defense against network intrusion and are best committed to memory. The password above is an example of a password that can be easily remembered. You must protect your password to reduce the risk of a security violation.

4. PROTECTING YOUR WORKSTATION

A. LOGGING OFF AND LOCKING YOUR WORKSTATIONS

- For security reasons, you should activate the ‘lock’ on your workstation when you leave it unattended for any period of time. To lock your workstation, press the ‘ctrl, alt, delete keys simultaneously and then click Lock Computer.
- Unless you are notified otherwise, you should at the end of each day click “log off” using similar steps as above, but you should not turn off the power to your workstation. Student Affairs Information Technology (SAIT) uses the after hours to update workstations with security patches and updates to your software. Please check our website at http://studentaffairs.psu.edu/ for notices of changes to this procedure.

B. SOFTWARE INSTALLATION

- In the majority of the cases, you will not be able to install software on your workstation without the support of SAIT. Because your workstation is for work related activities, it is very important that Student Affairs and the University be protected against malicious attacks that are often hidden in software that can be loaded on our workstations.
- SAIT must also ensure that software licensing agreements and University policy are in compliance.

5. ASSETS – USE AND HANDLING

A. OWNERSHIP

- Institutional Data
  - Databases, spreadsheets, documents and images created on servers or in workstation applications and stored on the servers or local hard disks are considered to be the property of the Division of Student Affairs and Penn State University.
  - AD53 – Privacy Statement explains the level of privacy that you should expect relating to e-mails etc.
6. NETWORK MANAGEMENT
   A. University Policy **AD20 Computer and Network Security** explains in detail the role of System Administrators – In brief, during the course of performing the position responsibilities, a Systems Administrator, “…have the same responsibilities as all system users”. They must treat the files of user as private. Prepare and maintain security procedures according to University and Division security policies. “It is recognized that a system administrator may have incidental contact with system user files, including electronic mail, in the course of his or her duties. The contents of such files must be kept private. Deliberate access to system user files is authorized only in the event of a suspected security breach, if essential to maintain the system(s) or network(s) for which the system administrator has direct administrative responsibility, or if requested by or coordinated with the system user.”

7. FILES AND DATA
   A. Shared files – Informational assets created by others on the Student Affairs network or informational assets that are accessed via the network (example - from AIS or the Internet) are to be used in accordance with applicable state and federal laws and Penn State policies.
   B. University data – The use of Penn State’s institutional data is strictly regulated and is only available to authorized users for appropriate educational purposes. Please refer to University policy **AD23**. It states that each employee “must recognize the importance of institutional data to the conduct of the University's mission, and take action to resolve or report to their management instances in which confidential institutional data are at risk of unauthorized disclosure, dissemination or destruction.”

8. HARDWARE AND SOFTWARE
   A. COPYING SOFTWARE
      • University Policy **AD20** states the following: Computer software protected by copyright is not to be copied from, into, or by using University Computer and Network Resources, except as permitted by law or by the license or contract with the owner of the copyright.
   B. HARDWARE CONFIGURATION
      • SAIT does not permit the modification of your workstation or the software that is installed. Your workstation is provided for the purpose of doing work for the Division and the University. If your position requires special configurations or special software, you can contact SAIT.
   C. YOUR WORKSTATION’S DESKTOP.
      • Student Affairs staff members are encouraged to personalize your workstation desktop. You may change the color and screen resolution of workstation monitors as well as personal desktop and application settings as long as these changes do not interfere with shared operation in the network environment and are not of an inflammatory nature.
      • A standard password protected screensaver is provided as a security feature.
9. ASSET MANAGEMENT
   A. All Computer equipment is listed in an asset tracking system for identification and
      tracking purposes. For your protection and the protection of our valuable equipment, you
      are required to contact SAIT prior to any relocation of equipment.
   B. Workstations and peripheral equipment purchased in the Division of Student Affairs is
      the property of the Division and not the Units. The equipment is controlled by SAIT and
      assigned based on need.

10. PERSONAL USE
    A. COMMERCIAL BUSINESS
       • It is not permitted to use any Division resources in conducting a business
         enterprise not specifically related to the Pennsylvania State University.
    B. PERSONAL USE AND PROJECTS
       • With the consent of your supervisor and the director of your department, you are
         welcome to work on personal projects as long as you are working on your own
         non-PSU time. Your management team is free to use full management discretion
         and may choose to prohibit you from working on personal projects using Student
         Affairs computer equipment. Each request will be reviewed on a ‘case by case’
         basis. Documents or images created as part of a personal project can be saved to
         a DVD, CD or a thumb drive, but must not to be stored on server disk space.
         You are permitted to store your personal information on the Penn State Access
         Account Storage Space (PASS) at http://its.psu.edu/PASS/. Use of printers for
         personal projects must also be kept to a minimum and must be approved as above.
         Personal use of your Penn State University access account and e-mail account is
         authorized providing such use does not violate any state or federal laws and
         conforms to existing computing policies enacted by The Pennsylvania State
         University and the Division of Student Affairs.

11. NETWORK DOWNTIME
    A. It is normal that there are times that network maintenance will be required. Those times
       will normally be during off-peak hours and will be announced prior to the downtime.
       There are occasions where unexpected downtime will occur. We are working to reduce
       those unexpected outages.

12. WEB BROWSING
    A. You are encouraged to restrict your personal use of network applications during your
       workday. Browsing the Web for business or personal use can substantially diminish
       work productivity as well as increase the possibility of receiving spam, viruses, malware
       and other undesirable items. Your supervisor can request that there is a restriction placed
       on your personal use of network services.
    B. At this time, SAIT only supports Internet Explorer as our browser.
13. INSTANT MESSENGER
   A. Security is a key component of providing network services to the Division of Student Affairs and the University. To prevent security breaches on the Student Affairs network, you will be unable to download, install or use any form of instant messaging applications such as Yahoo Messenger, AOL Instant Messenger, MSN Messenger, or other similar software. If found during security scans, instant messenger applications will be removed from any computers.

14. PERSONAL SOFTWARE
   A. Personal software will not be loaded on Student Affairs workstations unless there is a business reason. Supervisor approval must be given and SAIT must approve the software for its safety to operate on the Student Affairs network.

15. SECURITY
   A. HACKING AND VIRUSES
      • As a Student Affairs staff member it is your duty to help protect our work environment. It is your obligation to notify SAIT immediately in the event that you know or suspect that your network account or workstation has been compromised (by a virus or there has been an unauthorized access). SAIT has an obligation to remove and evaluate the workstation.
   
   B. UNAUTHORIZED ACCESS
      • Attempting to access systems or network resources for which you are not authorized is a security violation. Disciplinary action can be taken if this occurs. Please refer to our AD20 or our section on Policy Abuse for additional information.

   C. PHYSICAL SECURITY
      • We highly recommended that you protect Student Affairs’ inventory by closing and locking office door during non-business hours.

REFERENCES AND OTHER APPLICABLE POLICIES

AD08 - Purchase of Advertising
AD11 - University Policy on Confidentiality of Student Records,
AD20 - Computer and Network Security
AD23 - Use of Institutional Data,
AD27 - Commercial Sales Activities at University Locations,
AD53 - Privacy Statement,
AD56 - Use of Group E-Mail to Communicate University Business to Employees and Students,
AD35 - University Archives and Records Management,
ADG01 - Glossary of Computerized Data and System Terminology,
ADG02 - Computer Facility Security Guideline,
FN14 - Use of Tangible Assets, Equipment, Supplies, and Services, and
HR60 - Access to Personnel Files.

APPENDIX “A” – UHS ACCESS AND SECURITY BELOW
COMPUTERIZED INFORMATION SYSTEMS
ACCESS AND SECURITY

Purpose:

To outline UHS policy on employee use and access of UHS and PSU information systems. To outline penalties relating to violations of this policy. To state policies pertaining to the security of computers and data within UHS. Also, to state policies pertaining to unauthorized copying of software and copyright infringement.

Violations:

Violators of this policy may be denied access to UHS and PSU information systems, and may be subject to disciplinary action up to and including termination. In addition, violators may be subject to penalties under Federal, State, and PSU regulations.

Security of the UHS Network and PSU AIS
The UHS Network Administrator in the IS (Information Systems) office, in cooperation with Student Affairs IS, is responsible for maintaining the security of the UHS network, computers, and servers. The security is maintained and monitored in close cooperation with the PSU Computer Security and Operations Office, PSU Privacy Office, and the UHS Health Information Systems Committee. This policy corresponds to all Penn State, State, and Federal regulations.

Granting, Changing, and Terminating Access for Employees
UHS employees with a need for access to the UHS network and systems must first be given adequate training, user IDs, passwords, and security clearance by the Network Administrator.

Security determines what a user will be able to access. To the extent possible, security is granted on a "need to know" basis, according to what is necessary for the employee to fulfill his or her job requirements. Due to system limitations, it may be necessary to give a user access to components not required for job performance, in order to provide the required access. In this situation, the user should not attempt to make use of the system components which are not job related.

Supervisors must complete the “Software Access Request” form for employees under the following conditions:

- A new employee is hired
- An employee’s job functionality changes
- An employee leaves or is terminated

All UHS employees with computer access must read this policy and the following policies:

AD-20 Computer and Network Security
AD-23 Use of Institutional Data
ADG-1 Glossary of Computer Data and System Terminology
ADG-2 Computer Facility Security Guideline
All other associated PSU Policies
In addition, all employees must sign and abide by the “UHS Privacy and Security Agreement” form.

**UHS Information System Set-Up and Maintenance**

The Network Administrator is responsible for maintaining UHS information system parameters, defaults, code files, security clearances, and data security.

**System Error Messages and System Crash Recovery**

All computer system error messages and system crashes must be reported to the IS office immediately for analysis and resolution.

**Computer Software Copyrights**

All employees using copyrighted software, such as Microsoft Office, etc., must adhere to all copyright and licensing restrictions including those regarding the illegal copying of software.

**Disposal of Computer Media**

All computer media (disks, hard drives, memory cards, portable media storage devices, etc) should be given to IS for disposal. Disposal shall only occur after the media has been sanitized by Degaussing or other method approved by the PSU Privacy Office, and meeting the requirements of HIPAA and Department of Defense and/or NATO standards.

**Computer Security**

Users are responsible for any data additions, deletions, or modifications done under any of their computer ID’s. The various UHS and PSU systems will automatically prompt users to change their passwords when it is necessary to do so. Passwords should not be shared or posted in a conspicuous place. Passwords should be at least six characters in length, contain both letters and numbers, and should not be easily guessed by others.

Computer equipment, tapes, disks, and approved portable media storage devices should be kept physically secure at all times.

Employees should take measures to prevent infection of their computers by software viruses. Software viruses are programs that can damage data or computer hardware. Viruses are usually spread by files in infected disks or email attachments. Employees should know the source of any files they use. Employees that use files from outside sources should have an anti-virus program check the files for infection before use.
All computers must have anti-virus software installed. Employees must not download or install software on their computers without first contacting the IS office.

The following summarizes the above policies and outlines additional recommendations that computer users should follow:

- Users are responsible for any data entry that is done under their user account.
- Users should not share their passwords with anyone.
- All computer system error messages should be reported to the IS office immediately.
- IS must have a valid license for all software being used within UHS. Contact IS to install any new software on your computer and verify that it is licensed properly.
- Computer equipment, tapes, disks, etc., should be kept physically secure at all times.
- Know the source of any disk or email attachment you use. Use an anti-virus program on all outside disks or email attachments before using them.
- Users should store all data on shared network drives (i.e. – H or J), so that data is secure and backed up nightly.
- If you spill something into your computer or printer, please unplug it and call IS immediately.
- Please contact IS before moving any computer equipment.
- All computer media should be given to IS for proper sanitization and disposal.
- Magnets or anything with a strong electromagnetic field can damage computers, and should not come into close contact with any computer equipment.
- All computers and laser printers should be plugged into a surge suppressor or UPS (uninterruptible power supply) unit.
- When leaving your computer, you should lock it by pressing Control, Alt, Delete.
- All computers should be equipped with password protected screen savers.
- If you suspect that your computer, system access, or passwords have been used inappropriately, immediately contact IS or the chair of the UHS Health Information Systems Committee.
- Computers screens should be guarded from the public. When not actively using your computer, keep your screen on a menu or some other screen that does not contain confidential information. You may want to consider installing a privacy filter for computer screens that can be easily seen by the public.

- If you see or know of anything that may compromise UHS computer security, please contact the Chair of the UHS Health Information Systems Committee.

Origination Date: 8/20/94

Reviewed by:___________________________________________  Date:  2/20/09