College of Agricultural Sciences --- Acceptable Computer Use Policy: ITP-001

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment within the College of Agricultural Sciences.

2.0 Scope

This policy applies to faculty, educators, staff, students, contractors, consultants, temporary employees, and other workers in the College of Agricultural Sciences, including all personnel affiliated with third parties. This policy applies to all equipment that is connected to the College of Agricultural Sciences network.

3.0 Background

Inappropriate computer use exposes everyone to risks including virus attacks, compromise of network systems and services, and possible litigation. College computing systems are for business purposes in serving the administrative, academic, outreach, and research activities of the College, University, faculty, educators, staff and students.

Effective security is a team effort involving the participation and support of every College of Agricultural Sciences' employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly.

4.0 Policy

4.1 General Use and Ownership

1. The College recommends that any information that users consider sensitive or vulnerable be encrypted.
2. For security and network maintenance purposes, authorized individuals within the College of Agricultural Sciences may monitor equipment, systems and network traffic at any time, per the College of Agricultural Sciences' Audit Policy (ITP-003).
3. All software installed on college computers must have the appropriate software licenses. Any software not under college or university licensing must have the license registered with the user's budgetary office. All software and licenses are subject to college and university audit.
4. Computers purchased through Penn State University, including those that are grant funded are considered university assets and as such are accountable as inventory through the user's budgetary unit.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified according to the University data classification guidelines: Public, Internal/controlled, and Restricted. Currently (3.19.2009) definitions and examples can be found at: https://wikispaces.psu.edu/display/DCRFC/Penn+State+Data+Classification+Levels Employees should take all necessary steps to prevent unauthorized access to this information in accordance to the Penn State Minimum Security Standards currently (3.19.2009) available at: https://wikispaces.psu.edu/display/DCRFC/Penn+State+Minimum+Security+Standards .
2. All passwords and accounts should be secured and not shared. Authorized users are responsible for the security of their passwords and accounts. In addition to the password requirements listed in the College of Agricultural Sciences Password Policy (ITP-002), it is strongly recommended that system level passwords should be changed quarterly, and user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with passwords for all user accounts in compliance with the College of Agricultural Sciences Password Policy. Use additional settings as deemed necessary to prevent unauthorized access to resources and data.

4. All PCs, laptops and workstations that have security logging capabilities must have basic OS level auditing turned on to facilitate tracking of user accounts in the event of a security breach or other unauthorized access.
5. Because information contained on portable and remote computers is especially vulnerable, special care should be exercised. Portable and systems containing sensitive university data should utilize hard drive encryption techniques to protect the data in the event of unauthorized physical access to the system.
6. All hosts used by the employee that are connected to the College of Agricultural Sciences Internet/Intranet/Extranet, whether owned by the employee or the College of Agricultural Sciences, should be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when opening unsolicited e-mail attachments, which may contain viruses, e-mail bombs, or Trojan Horse code.
8. All systems connected with the College of Agricultural Sciences network infrastructure may only use IP addresses assigned by the College or its delegates. Any departments providing IP addresses via DHCP must employ a mechanism to ensure that only the intended host receives the IP address or are authenticated and logged so that the user of that IP address during a given period of time can be determined in the event of a security incident.
9. To maintain proper data encryption, all systems storing or utilizing sensitive administrative data, and using a wireless connection must also utilize a College approved VPN (virtual private network). Systems transferring sensitive university data over non-secure networks (wired or wireless) must encrypt that data during transmission.

4.3 Unacceptable Use

Under no circumstances is an employee of the College of Agricultural Sciences authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College of Agricultural Sciences-owned resources.

The following activities are prohibited except for certain exemptions as identified under Section 3.1, General Use and Ownership or specified in College Audit Policy ITP-003. The list is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

4.4 Prohibited System and Network Activities

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College of Agricultural Sciences.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College of Agricultural Sciences or the end user does not have an active license is strictly prohibited.
3. Employees are not permitted to store, or capture Personal Identifiable Information (PII) on any university-owned computer or any computer used for university work without an AD19 exception issued by the Office of Risk Management. The college, in cooperation with university Security Operations Services will conduct periodic PII scans to assist users detecting the presence of PII. If such information is found, college or departmental IT staff will notify the user. It is the users responsibility to remove the PII immediately.
4. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate College security officer should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a College of Agricultural Sciences computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any College of Agricultural Sciences account. Or, offers of products, items, or services for personal profit from any College of Agricultural Sciences account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. The only exception to this is when access is part of a security analysis performed by an authorized individual within the College or University. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
10. Port scanning or security scanning is expressly prohibited unless prior approval is obtained from the College Network Security office.
11. Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account apart from assigned duties performed by IT professionals.
13. Interfering with or unsanctioned denying of service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet apart from assigned duties performed by IT professionals.

4.5 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through content, language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or "pyramid" schemes of any type.
6. Use of unsolicited email originating from within The College of Agricultural Sciences's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the College of Agricultural Sciences or connected via The College of Agricultural Sciences's network.
7. Posting identical or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

6.0 Supporting Documents

College policy ITP-002 CAS Password Policy
College policy ITP-003 CAS Audit Policy
University policy AD20 Computer and Network Security

7.0 Revision History

Last updated: 12/14/2009

7.0 Employee's Confirmation

I have read, understand, and agree to comply with the provisions set forth in this policy.

_____ _____

Signature Date

_____ _____

Name (Please Print) PSU Access Account