College of Agricultural Sciences --- Audit Policy: ITP-003

1.0 Purpose

The purpose of this policy is to provide the authority for members of the College's security team and the University's Security Office to conduct security audits on any system within the College of Agricultural Sciences in accordance with University policy AD20 and College IT policy ITP-001.

2.0 Scope

This policy covers all computers and communication devices owned or operated by the College of Agricultural Sciences. This policy also covers any computer and communications devices that are not owned or operated by the College of Agricultural Sciences but are present on the College of Agricultural Sciences' network.

3.0 Policy

Members of the College or University security team are authorized to conduct security auditing upon direction of the University Security Operations Services office, the University Office of Risk Management, or University legal counsel. This authority may be delegated down to a departmental support team member upon approval by the College or University security team. Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Investigate possible security incidents and ensure conformance to the College of Agricultural Sciences security policies
3. Monitor user or system activity where appropriate (e.g. system compromise is suspected, policy violations are suspected, or complaints have been received).
4. Ensure validity of user accounts.

Users and/or support personnel must ensure that any hardware or software installed for the purposes of filtering traffic such as a firewall appliance or personal firewall software allow unrestricted traffic to and from all systems authorized to conduct security audits at the departmental, College and University Security Office levels. At no time shall anyone other than those authorized in the College or University be permitted to scan computers or devices connected to the College network. Any question as to the scope of addresses to be given unrestricted access can be directed to ITS at security@cas.psu.edu. This access may include:

1. User level and/or system level access to any computing or communications device
2. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the College of Agricultural Sciences equipment or premises
3. Access to work areas (labs, offices, cubicles, storage areas, etc.)
4. Access to interactively monitor and log traffic on the College of Agricultural Sciences networks.

4.0 Enforcement

Anyone found violating this policy will be subject to disciplinary action by his or her Administrative unit, the College, or the University. College or University Security Office personnel will immediately block Internet access to any system found to be scanning systems in violation of this policy. Individuals found to be in violation of local, Commonwealth or Federal regulations or laws will be referred to the University Security Office for case disposition.

5.0 Supporting Documents

6.0 Revision History

Last updated: 12/14/2009