Audit Policy
COE–AAP–AD20

1.0 Purpose
To provide the authority for members of the College’s security team and the University’s Security Office to conduct a security audit on any system within the College of Engineering in accordance with University policies. This authority may be delegated down to a departmental support team member upon approval by the College’s security team. All requests for such approval must originate from the department head in an email address to security@engr.psu.edu; ECS personnel will verify the authenticity of all emails before granting a request. Only approved departmental personnel will be authorized to scan systems within their department.

Audits may be conducted to:
- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents and ensure conformance to the College of Engineering security policies
- Monitor user or system activity where appropriate (e.g. system compromise is suspected, policy violations are suspected, and complaints have been received).
- Ensure validity of user accounts.

2.0 Scope
This policy covers all computer and communication devices owned or operated by the College of Engineering. This policy also covers any computer and communications devices that are present on the College of Engineering premises and network, but which may not be owned or operated by the College of Engineering.

3.0 Policy
When requested, and for the purpose of performing an audit, any access needed will be provided to members of College or University security teams. 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 ECS at security@engr.psu.edu.

This access may include:
- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the College of Engineering equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on the College of Engineering 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 Revision History
Last updated: 12/18/2009