Smeal College of Business - Audit Policy: SCB–AP–AD20

1.0 Purpose
To provide the authority for members of the College's I.T. security team and the University's Security Office to conduct security audits on any system within the Smeal College of Business in accordance with University policy AD20. Only approved RIIT Group network personnel will be authorized to scan systems within the Smeal College of Business.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents and ensure conformance to Smeal College of Business security policies
- Monitor user or system activity where appropriate (e.g. system compromise is suspected, policy violations are suspected, complaints have been received, activity is causing significant system or network degradation).
- Ensure validity of user accounts.
- Ensure conformance with the Smeal College of Business *Password Policy*

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

3.0 Policy
When requested, and for the purpose of performing an audit, server, system or account access will be provided to designated members of the Smeal 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 software firewall be configured to allow unrestricted traffic to and from all systems authorized to conduct security audits at the 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 Smeal College of Business network.

Any question as to the scope of addresses to be given unrestricted access can be directed to the Smeal College of Business RIIT Group networking team. 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 Smeal College of Business equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Smeal College of Business networks.

4.0 Enforcement

The Smeal College of Business Research Instructional and Information Technology Group (RIIT Group) has been authorized by the Dean of the Smeal College of Business to enforce this policy.

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 and LAN 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

06/04/2007 - Initial modification from COE policies, used with permission in conjunction with the Penn State IPAS project. http://www.ipas.psu.edu/