Smeal College of Business - Server Security Policy: SCB–SSP–01

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the Smeal College of Business, including servers operated at the departmental level for research purposes. Effective implementation of this policy will minimize unauthorized access to Smeal College of Business proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by all agents of the Smeal College of Business, and to servers registered under the Smeal College of Business network domain (smeal.psu.edu).

This policy applies specifically to equipment on internal Smeal College of Business networks including administrative systems as well as student and research labs.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at the Smeal College of Business must be owned by academic, research or other operational groups within the College and will have a designated person or persons who will be responsible for system administration. Approved server configuration guidelines must be established and maintained by each group, based on business needs and approved by the Dean's Office. Groups should monitor configuration compliance and implement a policy tailored to their environment. Each operational group must establish a process for changing the configuration guidelines, which includes review and approval by the Dean's Office and/or the College's IT department. All internal policies must be reviewed and approved by the Dean's Office or the Dean's designated representative.

3.2 General Configuration Guidelines

- Operating System configurations should be in accordance with approved College guidelines to ensure a significant level of security against unauthorized access.
- Services and applications that will not be used must be disabled, where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, software firewalls or other security mechanisms.
- The most recent security patches must be installed on the system within 48 hours of release. The only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk; their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Do not implement security procedures that will interfere with or block access from designated security teams within the College or University.

- Do not use a privileged account when a non-privileged account will do.
- If a methodology for secure channel connection is available and technically feasible, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment. Access to these areas should be traceable and auditable.
- Servers are specifically prohibited from operating in areas accessible to persons other than the intended system administrators.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 month.
    - Archived logs will be retained for a minimum of 1 year.
- Security-related events will be reported to College's Security team and/or Dean's Office, who may review logs and report incidents to the University Security Office. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Dictionary attacks
    - Unauthorized network scanning
    - Denial of service attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.
- Corrective measures may include:
    - Full system audit (including confiscation)
    - Disconnection from the network
    - Complete system rebuild
    - Disciplinary action

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within the Smeal College of Business or Penn State University.
- Audits will be managed by the University Security Office or College, in accordance with the Smeal College of Business *Audit Policy*. The College will present pertinent findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

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.

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University. Systems involved with severe security breaches may be confiscated for forensic analysis.

5.0 Definitions

Term	Definition
Server	For purposes of this policy, this is defined as a server internal to the Smeal College of Business providing services approved by the RIIT Group or Dean's Office. Desktop machines and Lab equipment are not germane to the scope of this policy unless providing some service to the network traditionally handled by a server (web server, ftp server, file share, etc.).
Denial of service attack	An attack designed to prevent a system from providing services to its users.
Dictionary attack	The automated use of a 'dictionary' of potential passwords used to attempt the compromise an account or a series of accounts.

6.0 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/