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 College of Engineering, including servers operated at the departmental level. Effective implementation of this policy will minimize unauthorized access to College of Engineering proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by all agents of the College of Engineering, and to servers registered under the College of Engineering-owned internal network domain.

This policy is specifically for equipment on the internal College of Engineering network including administrative systems as well as student and research labs.

3.0 Policy

3.1 Ownership and Responsibilities
All internal servers deployed at the College of Engineering must be owned by an academic, research or any other operational group that is 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 College. 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 must 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 must be logged and/or protected through access-control methods such as TCP Wrappers 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.
- Least privilege must be in effect at all times and administrative level accounts only used when necessary.
- 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 must be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating in areas accessible to persons other than the intended system administrators.
- Servers not needing to be accessed from outside the University should use private IP space to further isolate them from possible attack.
- Servers must run College approved antivirus, antispyware, firewall, and IDS software (if available and technically feasible) and keep all definitions and patches up-to-date.
3.3 Monitoring

- By University policy and applicable laws, 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 one month.
  - Archived logs will be retained for a minimum of one year.
- Security-related events will be reported to the College, 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.

3.4 Compliance

- Audits can be performed at any time deemed prudent or necessary, by authorized organizations within the College of Engineering.
- These audits will be managed in accordance with the 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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>For purposes of this policy, this is defined as a server internal to the College of Engineering providing services approved by ECS or the department. Desktop machines and Lab equipment are not germane to the scope of this policy.</td>
</tr>
<tr>
<td>Denial of service attack</td>
<td>An attack designed to prevent a system from providing services to its users.</td>
</tr>
<tr>
<td>Dictionary attack</td>
<td>The automated use of a ‘dictionary’ of potential passwords used to attempt the compromise an account or a series of accounts.</td>
</tr>
</tbody>
</table>

6.0 Revision History

Last Updated: 12/17/2009