Standard Title: Server Security
Standard Number: IS-S603
Responsible Office: Office of Information Security

Many *units* house *servers* that contain mission critical and/or *confidential university data*. It is important for these *servers* to have the highest level of security to protect the data. For the purpose of these standards, a *server* is defined as a system that provides services and resources to others. Desktop machines and lab equipment are not relevant to the scope of this standard.

The purpose of this section is to establish a baseline configuration of internal *server* equipment that is owned and/or operated by the university. Effective implementation of these standards will minimize unauthorized access to the university proprietary information and technology.

These standards apply to *server* equipment owned and/or operated by the university, and to *servers* registered under the university-owned internal *network*.

1. Ownership and Responsibility

All internal *servers* deployed at the university must be managed by an IT operational group that is responsible for system administration. Approved *server* configuration guidelines must be established and maintained by the IT operational group, based on business needs. *Information Security Liaisons/Managers* should monitor configuration compliance and document exceptions and alternative security measures used to secure these systems. The operational group must establish a process for keeping the configuration guidelines up to date.

Servers that house *confidential university data* must be registered with the Office of Information Security. At a minimum, the following information is required to positively identify the point of contact and pertinent *server* information:

- *Server* contact(s) and location, and a secondary contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Type of *confidential university data* housed on system
- Type and location of data backup

**The information listed above must be kept up to date in the central database to be developed by the university.

2. General Configuration

- Operating System configuration should be in accordance with approved university guidelines developed by the UISO and/or the CIO.
- 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, if possible.

- *Servers* should employ intrusion detection mechanisms, connection logging, and encryption technologies to the extent necessary to protect sensitive traffic.
- The most recent security patches must be installed on systems as soon as possible, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be carefully considered. A trust relationship must not be used when some other method of communication will do.
- Standard security principles of least access required to perform a function must always be used. Root or administrator MUST NEVER BE USED when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., 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. *Servers* are specifically prohibited from operating from desktop systems if services are offered outside the local network.
- Backup procedures must comply with the standards described in Business Continuity and Disaster Recovery Planning.

3. Monitoring

All security-related events on mission critical *devices* or *devices* containing *confidential university data*) must be logged and audit trails saved as follows:

- All security related *logs* will be kept for a minimum of 1 week.
- Daily backups of *logs* will be retained for at least 1 week.
- Weekly full backups of *logs* will be retained for at least 1 month.
- Monthly full backups of *logs* will be retained for a minimum of 1 year.
- Security-related events will be reported to the *UISO*, who will review *logs* and report *incidents* to the *CIO*. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-*scan attacks*
  - Evidence of unauthorized access
  - Anomalous occurrences that are not related to specific applications on the host.

4. Compliance

- Server audit logs, access reports and security incident tracking reports will be maintained and reviewed on a regular basis, as indicated in the Information Security Activity Review Guideline (IS-G603).
- Audits will be performed on a regular basis by authorized organizations within the university.
- Compliance with the policy is subject to periodic audit or review, or both. Audits will be managed in accordance with university policies and procedures. The Information Security Office will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

Related Guidance
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)

Exceptions Procedure (IS-P100)
Network Security Standard (IS-S600)
Server Scanning Procedure (IS-P603)
Information Security Activity Review Guideline (IS-G603)

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	08/09/07
Effective Date	05/27/08
Revised Version	04/17/12
Effective Date	10/31/12