Stony Brook University
Computer Science

Server Security Policy

CS Department Server Security Policy

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 SUNY Stony Brook CS department. Effective implementation of this policy will minimize unauthorized access to SUNY Stony Brook CS department proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by SUNY Stony Brook CS department, and to servers registered under any SUNY Stony Brook CS department-owned internal network domain.

This policy is specifically for equipment on the internal SUNY Stony Brook CS department network. For secure configuration of equipment external to SUNY Stony Brook CS department on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at SUNY Stony Brook CS department must be completely controlled by the CS department system staff. Approved server configuration guides must be established and maintained by the CS department systems staff, based on business needs and approved by Director of Labs. Director of Labs should monitor configuration compliance and implement an exception policy tailored to the production environment. Any/all operational group(s) must establish a process for changing the configuration guides, which includes review and approval by Director of Labs.

Servers must be registered within the department enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

Information in the department enterprise management system must be kept up-to-date.

Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

Operating System configuration should be in accordance with approved Director of Labs guidelines.

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.

The most recent security patches must be installed on the system as soon as practical, 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 avoided. Do not use a trust relationship when some other method of communication will do.

Always use standard security principles of least required access to perform a function.

Servers that provide file sharing should utilize an access control list for hosts that may access filesystems. The access control list should enumerate the clients allowed to access filesystems and avoid generalizations or wildcards in the list. Client systems should not be granted privileged access to shared filesystems

- Where possible, write protecting server filesystems is preferred. If possible, physically write protecting server filesystems is preferred over using software or OS supported mechanisms.
- Where possible, servers should be configured without default network routes or routes outside of production networks. Networks outside the working set of networks able to access a server should be unreachable.
- Servers should be powered from uninterruptible power supplies able to support the server for 10 minutes
- Do not use root 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 uncontrolled areas.

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 week.
  - Backups will occur at least 3 times a week on non-teaching lab server. 1 day per week on teaching lab servers.
  - Incremental tape backups will be retained for at least 3 months on non-teaching lab servers. Backups of teaching lab servers may be discarded 1 month after the close of a given semester.
  - Full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 1 year for non-teaching lab servers. Backups of teaching lab servers may be discarded 1 month after the close of a given semester.
  - 2 months old full backups from non-teaching labs will be stored offsite, in a fire resistant container with a key lock. The local storing agent will not possess a key to open the storage unit and will only turn the box over to the Director of Labs or an authorized, in writing, representative. Any person to whom the backup storage box is turned over to must present two picture identity cards one of which must be a current, valid Stony Brook id.
- Security-related events will be reported to the CS department systems staff and Director of Labs, who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized personnel within SUNY Stony Brook CS department.
- Audits will be managed by CS department systems staff or Director of Labs, in accordance with the *Audit Policy*. Director of Labs will filter findings not related to a specific operational group and then present the 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 users found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

Term	**Definition**
DMZ	De-militariezed Zone. A network segment external to the department production network.

Server	For purposes of this policy, a Server is defined as an internal SUNY Stony Brook CS department Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History