Stony Brook University
Computer Science

Host Security Policy

CS Department Host Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal host/client 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 host/client equipment owned and/or operated by SUNY Stony Brook CS department, and to host/clients 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 host/clients deployed at SUNY Stony Brook CS department must be completely controlled by the CS department system staff. Approved host/client configuration guides must be established and maintained by the CS department systems staff, based on business needs and approved by the Director of Labs. The 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 the Director of Labs.

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

- Host/client contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Special functions and applications, if applicable

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

Configuration changes for production host/clients must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

Operating System configuration should be in accordance with approved DOL 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. Do not configure general trust relations as part of the OS (e.g. hosts.equiv on Unix).

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

Where possible, write protecting host/client filesystems is preferred. If possible, physically write protecting host/client filesystems is preferred over using software or OS supported mechanisms.

Where possible, host/clients should be configured without default network routes or routes outside of production networks. Networks outside the working set of networks able to access a host/client should be unreachable.

- Idle console logins should invoke a password protected screen saver or logout the console user after 10 minutes of idle time where possible. There are sources on the Internet for idle login programs.
- It is preferable that all remote access occur over secure channels (e.g., encrypted network connections using SSH or IPSec). Access from outside the production CS department networks must occur over secured channels.
- Host/clients must require a login and password for a user to gain access to the console. The authentication database should not be local to the system (e.g. passwd file) but from a central database (e.g. use NIS, NIS+, LDAP, Active Directory Service, Kerberos or an equivalent)
- The CPU case should be secured to prevent an intruder from replacing the boot drive with his/her own unit
- Host/clients should be in a room with restricted access (e.g. combination lock, swipe card lock or key lock with a door that automatically remains locked when the key is removed from the lock)
- The system bios/boot manager should be password protected, if possible, to prevent reconfiguration of hardware settings/boot process.
- The system bios/boot monitor program should be configured to disallow booting from any device except the internal hard disk drive.
- Host/clients should be configured to disallow single-user booting or require a password to access the system if a single-user boot occurs
- Network connections should be secured to prevent removal or relocation to other systems except by authorized personnel.
- Removable media should never be mounted allowing a privileged program or a program that can assume privileged access to run.
- Host/clients should be powered from uninterruptible power supplies able to support the host/client for 10 minutes
- Systems running MS Windows/MS DOS must have the CS department standard virus scanning software loaded and running at all times. At no time may a client on a production network have the virus scanning software disabled. Refer to the CS department *Anti-virus Guidelines* for details.
- Removable media should always be virus scanned when the media is inserted into the media reader/system
- Do not use root or administrator accounts 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).
- Host/client OS's should never be configured on a network or network accessible from insecure networks. All care should be made to protect an OS distribution from being compromised prior to complete configuration and deployment.
- Host/client OS's should only be loaded from a secured copy of the OS. A secured copy of an OS is one that, due to physical limitations, cannot be altered once written onto the media (e.g. cdrom) or because the source has a continuous chain of possession in secured environments with no unauthorized persons able to access the media or device.
- Sufficient logging space on the local host/client or on a logging host should be available to retain 1 week of system logs.
- Refer to the CS department web site for additional FAQ's on host security issues.

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.
- 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
    - Evidence of unauthorized access to user accounts from the host/client
    - 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*. The 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 user 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.
Host/client	For purposes of this policy, a Host/client is defined as an internal SUNY Stony Brook CS department Desktop machine. Servers and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History