CS Department Internet Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal Internet 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 Internet server equipment owned and/or operated by SUNY Stony Brook CS department, and to Internet 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 Internet servers deployed at SUNY Stony Brook CS department must be completely controlled by the CS department system staff. Approved Internet 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.

> Internet 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:
> - Internet server contact(s) and location, and a backup contact
> - Hardware and Operating System/Version
> - Special functions and applications (e.g.: Netscape or Apache web server software, Sendmail SMTP server, DNS/BIND version xxx.xx)
>
> Information in the department enterprise management system must be kept up-to-date.
> Configuration changes for production Internet servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines
> Physical security should follow the *Server Security Policy*
> Software security should follow the *Server Security Policy*
> Internet servers should not mount general department filesystems where at all possible. It is preferable to replicate department filesystems, or subsets, onto a disk local to the Internet server in order to localize potential damage/violated filesystems to those local to the Internet server. Tools such as RDIST or RSYNC or MS Windows Directory Replication Service can be used to synchronize filesystems in one direction, to the Internet server.
> Internet servers should avoid user logins where at all possible. The authentication database should not be shared with the internal production network authentication system (e.g. NIS, or LDAP).
> 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 system on a production network have the virus scanning software disabled.

- The CS department Anti-virus Guidelines should be followed for MS Windows Internet servers.
- Internet server logging and backups should follow the *Server Security Policy*.
- 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 Internet server
    - 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-militarized Zone. A network segment external to the department production network.
Internet server	For purposes of this policy, a Internet server is defined as an internal SUNY Stony Brook CS department server machine. The machine provides services such as but not limited to: WWW, FTP, Electronic Mail, Web Email reading services, POP*, IMAP, Calendar. Desktop systems and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History