

DMZ Lab Security Policy

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in SUNY Stony Brook CS department labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to SUNY Stony Brook CS department from the damage to public image caused by unauthorized use of SUNY Stony Brook CS department resources, and the loss of sensitive/department confidential data and intellectual property.

2.0 Scope

SUNY Stony Brook CS department Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside SUNY Stony Brook CS department Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside SUNY Stony Brook CS department's Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ Labs must present a research or educational justification with sign-off with at least the Director of Labs. The systems staff will keep a record of the research/educational plan online.
2. Lab owning organizations are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must maintain up to date POC information with the systems staff and Director of Labs. Lab managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through the SUNY Stony Brook CS department systems staff and Director of Labs.
4. All ISP connections must be maintained by the SUNY Stony Brook CS department systems staff or the SUNY Stony Brook networking group in coordination with the CS department systems staff.
5. The DMZ Lab must maintain a firewall device between the DMZ Lab(s) and the Internet.
6. The CS department systems staff reserves the right to interrupt lab connections if a security concern exists.
7. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the CS department systems staff point of demarcation.
8. The CS department systems staff must record all DMZ Lab address spaces and current contact information and keep this information on the restricted department web site.
9. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of CS department systems staff upon request, in accordance with the *Audit Policy*
11. Individual lab accounts must be deleted within fourteen (14) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within fourteen (14) days from a change in the group membership.
12. The Director of Labs will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production systems or labs must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to SUNY Stony Brook CS department's internal networks, either directly or via a wireless connection.
3. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.

4. Lab Managers are responsible for complying with the following related policies:
 - a. *Password Policy*
 - b. *Wireless Communications Policy*
 - c. *Lab Anti-Virus Policy*
 - d. *Acceptable Use Policy*
5. The CS department systems staff maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by CS department systems staff.
6. The firewall device must be the only access point between the DMZ Lab and the rest of SUNY Stony Brook CS department's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by CS department systems staff (including both general configurations and rule sets). CS department systems staff may require additional security measures as needed.
8. Traffic from DMZ Labs to the SUNY Stony Brook CS department internal network, including VPN access, falls under the *Remote Access Policy*
9. No departmental services (password authentication, shared filesystems, printer services) or any system with direct access to these services may be directly accessed through the CS department firewall. Services or systems available to the general internet may be exempt.
10. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
11. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. See applicable FAQ's on the department secure web site.
12. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
13. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
14. Services and applications not serving educational or research requirements must be disabled.
15. SUNY Stony Brook CS department Confidential information is prohibited on equipment in labs where: Non-SUNY Stony Brook CS department personnel have unmonitored physical control or administrative access including students, RA, TA, PostDocs, visiting students, visiting faculty or other persons (e.g., training labs). Where, for any reason, CS department systems staff do not have unlimited physical access and remote access, in accordance with the *Information Sensitivity Classification Policy*
16. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.
17. Labs shall be placed into the DMZ when any person other than the CS department systems staff may require or have, for any period of time, administrative access to a system or communications device or where experimentation which may be disruptive to the CS department's production network may need to occur as part of the educational or research mission of the given lab.

4.0 Enforcement

Any user found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

Terms

Definitions

Access Control List (ACL) Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

DMZ (de-militarized zone) Networking that exists outside of SUNY Stony Brook CS department primary firewalls, but is still under SUNY Stony Brook CS department administrative control.

RA Research Assistant

<i>TA</i>	Teaching Assistant
<i>PostDoc</i>	Post Phd. Person who has earned a Phd and typically does not have a faculty position.
<i>Least Access Principle</i>	Access to services, hosts, and networks is restricted unless otherwise permitted.
<i>Internet Services</i>	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
<i>CS department systems staff Point of Demarcation</i>	The point at which the networking responsibility transfers from a CS department systems staff to the DMZ Lab. Usually a router or firewall.
<i>Lab Manager</i>	The individual responsible for all lab activities and personnel.
<i>Lab</i>	A Lab is any non-production environment, intended specifically for research, developing, demonstrating, training and/or testing of a product.
<i>Firewall</i>	A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by CS department systems staff.
<i>Internally Connected Lab</i>	A lab within SUNY Stony Brook CS department's firewall and connected to the department production network.
<i>Production Network</i>	That part of the CS department's network that is behind the firewall and is not used for experimentation and where users have the expectation of continuous availability and reliability of the systems connected to this part of the CS department network.

6.0 Revision History