DMZ Lab Security Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

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

2.0 Scope

<Company Name> Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside <Company Name> corporate 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 <Company Name>'s corporate 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 business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
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 InfoSec [and the corporate enterprise management system, if one exists]. 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 a <Company Name> Network Support Organization and approved by InfoSec.
4. All ISP connections must be maintained by a <Company Name> Network Support Organization.
5. A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.
6. The Network Support Organization and InfoSec reserve 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 Network Support Organization point of demarcation.
8. The Network Support Organization must record all DMZ Lab address spaces and current contact information [in the corporate enterprise management system, if one exists].
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 InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*

11. Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
12. InfoSec will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to <Company Name>'s corporate 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**
5. The Network Support Organization 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 InfoSec.
6. The firewall device must be the only access point between the DMZ Lab and the rest of <Company Name>'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 InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.
8. Traffic from DMZ Labs to the <Company Name> internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. [Add url link to site where your internal configuration standards are kept].
11. 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.
12. 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.
13. Services and applications not serving business requirements must be disabled.
14. <Company Name> Confidential information is prohibited on equipment in labs where non-<Company Name> personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. 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.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

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 <Company Name> primary corporate firewalls, but is still under <Company Name> administrative control.

Network Support Organization Any InfoSec-approved support organization that manages the networking of non-lab networks.

Least Access Principle Access to services, hosts, and networks is restricted unless otherwise permitted.

Internet Services Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.

Network Support Organization Point of Demarcation The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.

Lab Manager The individual responsible for all lab activities and personnel.

Lab A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.

Firewall A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.

Internally Connected Lab A lab within <Company Name>'s corporate firewall and connected to the corporate production network.

6.0 Revision History