Internal 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 <Company Name> labs to ensure that <Company Name> confidential information and technologies are not compromised, and that production services and other <Company Name> interests are protected from lab activities.

2.0 Scope
This policy applies to all internally connected labs, <Company Name> employees and third parties who access <Company Name>'s labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities
1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard <Company Name> from security vulnerabilities.

3. Lab managers are responsible for the lab's compliance with all <Company Name> security policies. The following are particularly important: *Password Policy for networking devices and hosts, Wireless Security Policy, Anti-Virus Policy, and physical security*.

4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The Network Support Organization must record all lab IP addresses, which are routed within <Company Name> networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

9. All user passwords must comply with <Company Name>'s *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains <Company Name> proprietary information, group account passwords must be changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-<Company Name> networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all <Company Name> product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with <Company Name>'s *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-<Company Name> personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no <Company Name> confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy.*

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to <Company Name> corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party 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

- Internal - A lab that is within <Company Name>'s corporate firewall and connected to <Company Name>'s corporate production network
- Network Support Organization - Any InfoSec approved <Company Name> support organization that manages the networking of non-lab networks.
- 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.
- External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of <Company Name> network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
- Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
- Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
- Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
- Extranet - Connections between third parties that require access to connections non-public <Company Name> resources, as defined in InfoSec's Extranet policy (link).
- DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under <Company Name> administrative control.

6.0 Revision History