Lab Security Policy

1. Overview

See Purpose.

2. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and Ilitera networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at Ilitera and its subsidiaries must adhere to this policy. This policy applies to Ilitera owned and managed labs, including labs outside the corporate firewall (DMZ).

4. Policy

4.1 General Requirements

4.1.1 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.

4.1.2 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 Ilitera from security vulnerabilities.

4.1.3 Lab managers are responsible for the lab's compliance with all Ilitera security policies.

4.1.4 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.

4.1.5 All user passwords must comply with Ilitera 's *Password Policy*.

4.1.6 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).

4.1.7 PC-based lab computers must have Ilitera's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

4.1.8 Any activities with the intention to create and/or distribute malicious programs into Ilitera's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

4.1.9 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.

4.1.10 In accordance with *the Data Classification Policy*, information that is marked as Ilitera Highly Confidential or Ilitera Restricted is prohibited on lab equipment.

4.1.11 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*.

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

4.2 Internal Lab Security Requirements

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

4.2.2 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.

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

4.2.4 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.

4.2.5 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.

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

4.2.7 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.

4.2.8 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.

4.2.9 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.

4.2.10 Lab owned gateway devices are required to comply with all Ilitera product security advisories and must authenticate against the Corporate Authentication servers.

4.2.11 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 Ilitera's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

4.2.12 In labs where non-Ilitera personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ilitera 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.

4.2.13 Lab networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

4.3 DMZ Lab Security Requirements

4.3.1 New DMZ labs require a business justification and VP-level approval from the business unit. Changes to the connectivity or purpose of an existing DMZ lab must be reviewed and approved by the InfoSec Team.

4.3.2 DMZ labs must be in a physically separate room, cage, or secured lockable rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.

4.3.3 DMZ lab POCs must maintain network devices deployed in the DMZ lab up to the network support organization point of demarcation.

4.3.4 DMZ labs must not connect to corporate internal networks, either directly, logically (for example, IPSEC tunnel), through a wireless connection, or multi-homed machine.

4.3.5 An approved network support organization must maintain a firewall device between the DMZ lab and the Internet. Firewall devices must be configured based on least privilege access principles and the DMZ lab business requirements. Original firewall configurations and subsequent changes must be reviewed and approved by the InfoSec

Team. All traffic between the DMZ lab and the Internet must go through the approved firewall. Cross-connections that bypass the firewall device are strictly prohibited.

4.3.6 All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.

4.3.7 Operating systems of all hosts internal to the DMZ lab running Internet Services must be configured to the secure host installation and configuration standards published the InfoSec Team.

4.3.8 Remote administration must be performed over secure channels (for example, encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.3.9 DMZ lab devices must not be an open proxy to the Internet.

4.3.10 The Network Support Organization and InfoSec reserve the right to interrupt lab connections if a security concern exists.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

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

6 Related Standards, Policies and Processes

- Audit Policy
- Acceptable Use Policy
- Data Classification Policy
- Password Policy

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- DMZ
- Firewall

8 Revision History

Date of Change	Responsible	Summary of Change
September 2018	Ilitera Policy Team	Updated, made general lab and included DMZ lab requirements, and converted to new format.