Lab Security Policy

1.0 Purpose

Laboratory environments (labs) often require configurations and network access distinct from the standard corporate production environment, potentially introducing unique security risks. This policy establishes the information security requirements necessary to manage and safeguard lab resources, minimize the exposure of critical infrastructure and information assets, and protect the organization's networks from threats originating from or traversing lab environments. Its purpose is to ensure labs are operated securely, balancing operational needs with essential security controls.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers involved in the management, operation, or use of organizational labs. It covers all organization-owned and managed labs, including those located internally, externally, or within a Demilitarized Zone (DMZ), and applies to all associated systems, networks, equipment, hardware, software, and firmware within these lab environments.

3.0 Policy Statements

3.1 General Lab Management & Responsibility

*   **Ownership and Points of Contact (POC):** Each lab must have a designated owning organization/department, a primary Lab Manager, and at least one designated backup POC. Lab owners must register and maintain up-to-date POC information with the designated IT authority (e.g., Precision Computer) and relevant network/asset management teams. POCs (manager or backup) must be reachable for emergencies; otherwise, necessary security actions may be taken without their direct involvement.
*   **Lab Manager Accountability:** Lab Managers are accountable for the overall security posture of their lab, its compliance with all relevant organizational security policies (including this one), and its potential impact on other networks (corporate or external). They must implement procedures to ensure policy adherence and safeguard against vulnerabilities.
*   **Policy Compliance:** All activities within the lab must comply with applicable organizational policies, including but not limited to Acceptable Use, Data Classification, Password, and Audit Logging policies.
*   **Immediate Access for Security/Support:** Lab Managers must grant immediate access to lab equipment and system logs upon request to authorized personnel from the designated IT authority (e.g., Precision Computer) or Network Support Organization for security investigations or operational support.

3.2 Access Control

*   **Physical Access:** Lab Managers are responsible for controlling and managing physical access to their labs. Access shall only be granted to individuals with a documented, immediate business need. Access lists must be reviewed regularly, and access promptly terminated when no longer required.
*   **Logical Access:**
    *   Individual user accounts on lab devices must comply with the organization's Password Policy.
    *   Individual user accounts must be disabled or deleted within three (3) days of authorization removal.
    *   Passwords for shared or group accounts on lab systems must be changed at least quarterly and meet complexity requirements defined in the Password Policy.

3.3 Host and System Security

*   **Anti-Virus/Malware:** All PC-based lab computers capable of running such software must have organization-standard, supported anti-virus/anti-malware protection installed, configured for regular scans, and kept up-to-date (software and definitions). Infected systems must be immediately isolated from all networks until verified clean. Lab Managers must implement procedures to ensure this.
*   **Malicious Activity:** Intentionally creating or distributing malicious programs (viruses, worms, malware) is strictly prohibited, per the Acceptable Use Policy.
*   **Patching:** Systems within labs should be patched according to organizational vulnerability management standards, especially if connected to other networks. Systems that cannot be patched require compensating controls and potential isolation.

3.4 Data Security and Service Restrictions

*   **Prohibition of Production Services:** Labs must not host ongoing, shared, business-critical services that generate revenue or provide primary customer capabilities ("production services"). Such services must be managed by appropriate production support organizations.
*   **Data Classification Restrictions:** Information classified as Highly Confidential or Restricted (or equivalent high-sensitivity classifications per the Data Classification Policy) is generally prohibited on lab equipment unless the lab has specific approvals and security controls commensurate with that data sensitivity level.
*   **Audit Logging:** Lab systems must comply with the Audit Logging Policy where applicable, especially for systems connected to corporate networks or handling sensitive test data.

3.5 Internal Lab Network Security (Labs connected behind corporate firewall)

*   **Firewall Segregation:** All internal labs must be segregated from the corporate production network via a firewall managed by the designated Network Support Organization or IT authority.
*   **Network Monitoring and Intervention:** The Network Support Organization and/or designated IT authority (e.g., Precision Computer) reserve the right to monitor traffic and interrupt lab connections that negatively impact the corporate production network or pose a security risk.
*   **IP Address Management:** All lab IP addresses routed within organizational networks must be registered in the central IP address management system with current lab POC information.
*   **External Connections:** Adding direct external network connections (e.g., Internet, partner

networks) requires documented business justification, network diagrams, and formal review and approval by the designated IT authority (e.g., Precision Computer) *before* implementation.
*   **Prohibition of Cross-Connections:** Devices (wired or wireless) within the lab must not create unauthorized connections that bypass the designated firewall between the lab and production networks.
*   **Firewall Configuration Control:** Initial firewall configurations and subsequent changes require review and approval by the designated IT authority (e.g., Precision Computer).
*   **Prohibition of Disruptive Activities:** Labs must not engage in activities like unauthorized port scanning, network auto-discovery, or traffic flooding/spamming that could negatively impact corporate or external networks. Such testing must be contained strictly within the isolated lab environment.
*   **Inter-Lab Traffic:** Traffic between lab networks or between labs and production may be permitted based on approved business needs, provided it is properly secured (e.g., via firewall rules) and does not introduce unacceptable risk or negatively impact network performance. Labs must not advertise services that could conflict with production services.
*   **Auditing Rights:** The designated IT authority (e.g., Precision Computer) reserves the right to audit lab network traffic, configurations, and administration processes.
*   **Gateway Device Security:** Lab-owned gateway devices (routers, firewalls) must comply with relevant security advisories/patching requirements and should authenticate administrative access against central authentication servers where feasible. Enable/privileged access passwords must be unique, comply with the Password Policy, and be restricted to authorized administrators.

3.6 Security for Labs with Non-Organizational Personnel Access (e.g., Training Labs)

*   Labs where non-organizational personnel have physical access must *not* have direct connectivity to the corporate production network.
*   Organizational confidential information must not reside on systems within these labs.
*   Connectivity *from* these labs *to* the corporate production network for authorized personnel must use secure, authenticated methods approved by the designated IT authority (e.g., Precision Computer), such as client VPNs, SSH tunnels, or temporary authenticated access lists ('lock and key').

3.7 DMZ Lab Security Requirements

*   **Approval:** Establishing new DMZ labs requires strong business justification and executive (VP-level or higher) approval. Significant changes to existing DMZ lab connectivity or purpose require review and approval by the designated IT authority (e.g., Precision Computer Team).
*   **Physical Security:** DMZ labs must reside within physically secure, dedicated spaces (room, cage, or locked racks) with strictly controlled access lists maintained by the Lab Manager.
*   **Network Management:** DMZ lab personnel are responsible for managing network devices within the lab up to the demarcation point defined by the Network Support Organization.
*   **Prohibition of Internal Connections:** DMZ labs are strictly prohibited from having any direct or logical connection (e.g., IPsec tunnel, wireless bridge, multi-homed host) to corporate internal networks.
*   **Internet Firewall:** An approved firewall, managed by the Network Support Organization or IT authority, must exist between the DMZ lab and the Internet. Configurations must be based on the

principle of least privilege, reviewed and approved by the IT authority (e.g., Precision Computer Team), and all Internet traffic must traverse this firewall. Bypassing the firewall is prohibited.
* **Device Standardization:** Routers and switches within the DMZ lab (not used for testing) should conform to applicable organizational standards.
* **Secure Host Configuration:** Operating systems of hosts providing services within the DMZ must adhere to secure baseline configuration standards published by the designated IT authority (e.g., Precision Computer Team).
* **Secure Administration:** Remote administration must utilize secure, encrypted channels (e.g., SSH, IPsec VPN) or dedicated, out-of-band management networks.
* **No Open Proxies:** DMZ lab devices must not be configured as open proxies to the Internet.
* **Security Intervention:** The Network Support Organization and/or designated IT authority (e.g., Precision Computer) reserve the right to interrupt DMZ lab connections if a security risk is identified.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including network scans, vulnerability assessments, configuration audits, physical inspections (walk-thrus), review of access logs and procedures, internal/external audits, and investigation of security incidents.

4.2 Exceptions/Waivers

Requests for waivers or exceptions to this policy must be formally documented with business justification, risk assessment, and proposed compensating controls. Exceptions require review and advance approval by the designated IT authority (e.g., Precision Computer Team) on a case-by-case basis.

4.3 Enforcement

Non-compliant labs may face network isolation or disconnection. Failure by Lab Managers or personnel to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

* **DMZ (Demilitarized Zone):** A perimeter network segment logically placed between an internal network and an external network (like the Internet), designed to host external-facing services while protecting the internal network.
* **Firewall:** A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
* **Lab Manager:** The individual assigned primary responsibility for the operation, management, and security of a specific laboratory environment.
* **POC (Point of Contact):** An individual designated as a contact person for a specific lab or function.

*   **Production Services:** Ongoing, shared, business-critical IT services essential for core operations, revenue, or customer functions, typically managed under stricter change control and support agreements than lab environments.

6.0 Related Policies

*   Acceptable Use Policy
*   Audit Logging Policy
*   Data Classification Policy
*   Password Policy
*   Physical Security Policy
*   Remote Access Policy
*   Change Management Policy
*   Vulnerability Management Policy
*   Wireless Security Policy

Revision #2
Created 28 August 2024 16:54:11 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery