Acquisition Assessment Policy

1.0 Purpose

The purpose of this policy is to establish the framework and minimum security requirements for assessing and integrating newly acquired companies into the organization's environment. Integrating acquisitions can significantly impact the security posture of both entities due to differences in infrastructure, policies, and culture. This policy aims to manage these risks by defining a process to:

* Assess the acquired company's security landscape, posture, and practices.
* Protect both the parent organization and the acquired company from increased security risks during and after integration.
* Educate the acquired company's personnel on the organization's security policies and standards.
* Facilitate the adoption and implementation of the organization's security policies and standards within the acquired entity.
* Ensure secure integration of networks and systems.
* Establish requirements for ongoing monitoring and auditing post-acquisition.

This policy outlines the responsibilities of the designated IT authority (e.g., Precision Computer Team) and defines the minimum security baseline required before connecting acquired systems or networks to the organization's infrastructure.

2.0 Scope

This policy applies to all corporate acquisitions made by the organization. It pertains to all personnel, systems, networks, data, laboratories, test equipment, hardware, software, and firmware owned and/or operated by the acquired company that will be integrated or connected to the organization's environment.

3.0 Policy Statements

3.1 Acquisition Assessment and Integration Process

* **IT Authority Involvement:** The designated IT authority (e.g., Precision Computer Team) must be an active member of the corporate acquisition team from the outset and throughout the entire process.
* **Risk Assessment:** The IT authority is responsible for conducting thorough security

assessments of the acquired company to identify and evaluate information security risks related to their infrastructure, systems, applications, data handling practices, and overall security posture.
*   **Remediation Planning:** Based on the risk assessment, the IT authority will develop a remediation plan in collaboration with relevant parties from both the organization and the acquired company.
*   **Implementation:** The IT authority will work with the acquisition integration team to implement necessary security controls and remediate identified risks *before* establishing connectivity between the acquired entity's network and the organization's network.

3.2 Minimum Security Requirements for Integration

The following minimum requirements must be met by the acquired company before network integration, unless a formal, risk-accepted exception is granted:

*   **Hosts (Servers, Desktops, Laptops):**
    *   All end-user devices (desktops, laptops) must either be replaced with organization-standard equipment, re-imaged with the organization's standard operating environment build, or demonstrably meet all requirements outlined in the organization's endpoint security standards (e.g., Baseline Workstation Configuration Standard).
    *   All hosts must have organization-approved and updated endpoint protection (anti-virus/anti-malware) software installed and operational before network connection.
    *   Business-critical production servers that cannot be immediately replaced or re-imaged require a specific security audit and a formal waiver granted by the IT authority (e.g., Precision Computer Team). These servers must meet applicable organizational security standards for servers.
*   **Networks:**
    *   Network infrastructure devices (routers, switches, firewalls) within the scope of integration must typically be replaced with organization-standard equipment or reconfigured/re-imaged to meet organization standards.
    *   Wireless network access points must be reconfigured or replaced to comply strictly with the organization's Wireless Network Connection Standard. Unauthorized or insecure wireless networks must be disabled.
*   **Internet Connections:**
    *   Existing direct internet connections of the acquired company must generally be terminated post-integration, with internet access routed through the organization's controlled perimeter.
    *   Air-gapped or segmented internet connections required for specific, justified business needs must be reviewed and formally approved by the IT authority (e.g., Precision Computer Team).
*   **Remote Access:**
    *   All existing remote access solutions (VPNs, dial-up, etc.) of the acquired company must be terminated.
    *   Remote access for acquired personnel will be provisioned through the organization's standard, approved remote access solutions and policies.
*   **Laboratory Environments (If Applicable):**
    *   Laboratory networks must be logically and, where appropriate, physically segregated from corporate/production networks, typically using firewalls managed according to organizational standards.
    *   Physical access to lab environments must be secured and restricted based on organizational

physical security policies.
    * Any direct external network connections (e.g., to partners, customers) originating from labs must be reviewed, justified, and approved by the relevant security authority (e.g., Precision Computer Team or a specialized Lab Security Group ["LabSec"], if applicable).
    * All acquired labs must adhere to the organization's specific lab security policies/standards or obtain a formal waiver from the relevant authority ("LabSec" or IT Security).

3.3 High-Risk Acceptance

* In exceptional circumstances where critical business needs necessitate connecting acquired networks or systems that fail to meet these minimum requirements, the associated risks must be formally documented by the IT authority. Connection under such circumstances requires explicit acknowledgment and acceptance of the identified risks by the organization's Chief Information Officer (CIO) or another designated executive sponsor.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify the acquired company's compliance with these requirements through audits, configuration reviews, vulnerability scans, interviews, documentation review, and other assessment methods before and during integration. Ongoing compliance will be monitored post-integration.

4.2 Exceptions

As noted in sections 3.2 and 3.3, exceptions to specific requirements require formal documentation, risk assessment, justification, compensating controls (if applicable), and advance approval from the designated IT authority (e.g., Precision Computer team) or, for high-risk acceptance, the CIO.

4.3 Enforcement

Failure to meet these requirements may delay or prevent the integration of the acquired company's networks and systems. Continued non-compliance post-integration may result in disconnection or further remediation actions. Policy violations by personnel may be subject to disciplinary action according to the parent organization's policies.

5.0 Definitions

* **Business Critical Production Server:** A server hosting applications or services whose failure would significantly impact core business operations, revenue generation, or service delivery.
* **Air-gapped:** A security measure where a computer network or device is physically isolated from other networks, particularly unsecured ones like the public internet.

Revision #2
Created 28 August 2024 16:48:48 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery