Acquisition Assessment 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
To establish InfoSec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an InfoSec acquisition assessment.

2.0 Scope
This policy applies to all companies acquired by <Company Name> and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

3.0 Policy

I. General
Acquisition assessments are conducted to ensure that a company being acquired by <Company Name> does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. InfoSec will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The InfoSec role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to <Company Name>'s networks. Below are the minimum requirements that the acquired company must meet before being connected to the <Company Name> network.

II. Requirements
A. Hosts
1. All hosts (servers, desktops, laptops) will be replaced or re-imaged with a <Company Name> standard image.
2. Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by InfoSec.
3. All PC based hosts will require <Company Name> approved virus protection before the network connection.

B. Networks
1. All network devices will be replaced or re-imaged with a <Company Name> standard image.
2. Wireless network access points will be configured to the <Company Name> standard.

C. Internet
1. All Internet connections will be terminated.
2. When justified by business requirements, air-gapped Internet connections require InfoSec review and approval.

D. Remote Access
1. All remote access connections will be terminated.
2. Remote access to the production network will be provided by <Company Name>.

E. Labs

1. Lab equipment must be physically separated and secured from non-lab areas.
2. The lab network must be separated from the corporate production network with a firewall between the two networks.
3. Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group (LabSec).
4. All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec.
5. In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the <Company Name> Chief Information Officer (CIO) must acknowledge and approve of the risk to <Company Name>'s 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**
Business Critical Production Server	A server that is critical to the continued business operations of the acquired Company.