Acquisition and Merger Assessment Policy

Last Update Status: *Updated October 2022*

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

1. Purpose

1.1. The purpose of this policy is to establish our organization's responsibilities regarding corporate acquisitions and mergers. This policy also defines the minimum security requirements involved in the Information Security acquisition assessment.

2. Scope

2.1. 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

2.2. The process of integrating a newly acquired company can have a drastic impact on the security posture of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

2.2.1. Assess company's security landscape, posture, and policies.

2.2.2. Protect both <Company Name> and the acquired company from increased security risks.

2.2.3. Educate acquired company's team members about <Company Name> policies and standards.

2.2.4. Adopt and implement <Company Name> Security Policies

2.2.5. Integrate acquired company

2.2.6. Continuous monitoring and auditing of the acquired company.

3. Policy Statements

3.1. General

3.1.1. 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. The Information Security Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Information Security role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work along 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.

3.2. Hosts
- 3.2.1. All endpoints (servers, desktops, laptops) will be replaced or re-imaged with <Company Name> standard security baseline configuration and will be required to maintain this minimum standards.
- 3.2.2. Business critical production servers that cannot be replaced or re-imaged must be audited. There must be an exception granted and documented by the Information Security Team.
- 3.2.3. All end-point computing devices will require <Company Name> approved anti-virus protection and/or Endpoint Detection and Response software (EDR) before network connection is established.

3.3. Networks
- 3.3.1. All network devices will be replaced or re-imaged with a <Company Name> standard baseline configuration.
- 3.3.2. Wireless network access points will be configured to the <Company Name> standard baseline configuration.
- 3.3.3. The acquired company's network must comply with <Company Name> network standard security baseline configuration.

3.4. Internet
- 3.4.1. All Internet connections will be terminated.
- 3.4.2. When justified by business requirements, air-gapped Internet connections will require the Information Security Team's review and approval.

3.5. Remote Access
- 3.5.1. All remote access connections will be terminated.
- 3.5.2. Remote access to any production, test, development, or guest network will be provided by <Company Name>.

3.6. Labs
- 3.6.1. Lab equipment must be physically separated and secured from non-lab areas.
- 3.6.2. The lab network must be separated from the corporate production network with a Virtual network (VLAN) with a firewall between the two networks.
- 3.6.3. Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Information Security Team or the Lab Security Group (LabSec).
- 3.6.4. All acquired labs networks must conform with the LabSec standard security baseline configuration.
- 3.6.5. In the event the acquired networks and computer systems fail to meet these requirements, the <Company Name> Chief Risk Officer (CRO) must acknowledge and approve of the risk to <Company Name>'s networks.

4. Responsibility

4.1. The Chief Information Security Officer of our organization or a designee from the Governance committee who will oversee and sign off on these Information Security policies. In smaller organizations, this may be the Information Security Manager. All employees, volunteers, and contractors are responsible for reading, understanding and complying with our organization's information security policies.

5. Compliance and Exceptions

5.1. The Information Security Team (InfoSec Team) will verify compliance to this policy through various methods, including but not limited to, reports from business tools, external audits, internal assessments, and interaction with the policy owner.

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

5.3. An employee, volunteer, or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination.

6. Definitions and Terms

6.1. Terms and definitions can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/.

7. Revision History

Date of Change	**Responsible**	**Summary of Change**
Dec 2013	SANS Policy Team	Converted to new format and retired
July 2021	SANS Policy Team	Converted to new format.
October 2022	SANS Policy Team	Updated