Cybersecurity Policy Templates

Acquisition Assessment Standard

(Last Updated April 2025)

Purpose

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.

Scope

This policy applies to all <Company Name> employees and affiliates.

Safeguards

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. 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.

Hosts

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.

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.

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.

Networks

All network devices will be replaced or re-imaged with a <Company Name> standard baseline configuration.

Wireless network access points will be configured to the <Company Name> standard baseline configuration.

The acquired company's network must comply with <Company Name> network standard security baseline configuration.

Internet
All Internet connections will be terminated.

When justified by business requirements, air-gapped Internet connections will require the Information Security Team's review and approval.

Remote Access
All remote access connections will be terminated.

Remote access to any production, test, development, or guest network will be provided by <Company Name>.

Labs
Lab equipment must be physically separated and secured from non-lab areas.

The lab network must be separated from the corporate production network with a Virtual network (VLAN) with a firewall between the two networks.

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).

All acquired labs networks must conform with the LabSec standard security baseline configuration.

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.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.