1. Overview

1.1 The process of integrating a newly acquired company can have a drastic impact on the security poster 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.

- Assess company's security landscape, posture, and policies.
- Protect both Kinyo and the acquired company from increased security risks.
- Educate acquired company about Kinyo policies and standard
- Adopt and implement Kinyo Security Policies and Standards.
- Integrate acquired company.
- Continuous monitoring and auditing of the acquisition.

2. Purpose

2.1 The purpose of this policy is to establish I.T. team responsibilities regarding corporate acquisitions and define the minimum-security requirements of an I.T. team acquisition assessment.

3. Scope

3.1 This policy applies to all companies acquired by Kinyo and pertains to all systems, networks, laboratories, test equipment, hardware, software, and firmware, owned and/or operated by the acquired company.

4. Policy

4.1 General

4.1.0 Acquisition assessments are conducted to ensure that a company being acquired by Kinyo does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The I.T. teams will provide personnel to serve as active members of the acquisition team throughout the entire acquisition processes. The I.T. team role is to detect and evaluate information security risks, prior to allowing connectivity to Kinyo networks. Below are the minimum requirements that the acquired company must meet before being connect to the Kinyo network.

4.2 Requirements:

4.2.1 Hosts

4.2.1.0 All host (servers, desktops, laptops) will be replacing or re-imaged with a Kinyo standard image or will require to adopt the minimum standards for end user devices.

4.2.1.1 Business critical production servers that cannot be replace or re-imaged must be audit and a waiver granted by I.T. team.

4.2.1.2 All PC based host will require Kinyo approved virus protection before the network connection.

4.2.2 Networks

4.2.2.1 All network devices will replace or re-imaged with Kinyo standard image.

4.2.2.2 Wireless network access points will be configured to the Kinyo standard.

4.2.3 Internet

4.2.3.1 All internet connections will be terminated.

4.2.3.2 When justified by business requirements, air-gapped internet connections require I.T. team review and approval.

4.2.4 Remote Access

4.2.4.1 All remote access connections will be terminated.

4.2.4.2 Remote access to the production network will be provide by Kinyo.

4.2.5 Labs

4.2.5.1 Lab equipment must be physically separate and secured from non-lab areas.

4.2.5.2 The lab network must be separate from corporate production network with a security system between two networks.

4.2.5.3 Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be review and approved by I.T. team.

4.2.5.4 In the event the acquired networks and computer systems being connect to the corporate network fail to meet these requirements, the Kinyo I.T. Manager must acknowledge and approve of the risk to Kinyo networks.

5. Policy Compliance

5.1 Compliance Measurement

The I.T. team will verify compliance to this policy through various methods, including but not limit to, business tool reports, internet and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exceptions to the policy must be approved by the I.T. team in advance.