1. Overview

Remote access to our company network is essential to maintain our team's productivity, in cases this remote access originates from networks that may already be compromised or are at significantly lower security posture than our company networks. While these remote networks are beyond the control of Kinyo VA, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Kinyo's network from any external network. These rules and requirements designed to minimize the potential exposure to Kinyo from damages which may result from unauthorized use of Kinyo resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Kinyo internal systems, and fines, or other financial liabilities incurred because of those losses.

3. Scope

This policy applies to all Kinyo employees, contractors, vendors, and agents with a Kinyo owned or personally owned computer or workstation used to connect to the Kinyo network. This policy applies to remote access connections used to do work on behalf of Kinyo, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to Kinyo networks. This policy also applies to any device that has Kinyo data and is indirectly connected to any network such as removeable storage, remote printers, and remote IP telephones.

4. Policy

It is the responsibility of Kinyo employees, contractors, vendors, and agents with remote access privileges to Kinyo's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Kinyo.

General access to the Internet for recreational use through the Kinyo network is limited to Kinyo employees, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing the Kinyo network from a personal computer, Authorized Users are responsible for preventing access to any Kinyo computer resources or data by non-Authorized Users. Performance of illegal activities through the Kinyo network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy. Access to Kinyo's production network with personal devices (any non-guest networks) requires written permission from I.T. department.

***** Authorized Users will not use Kinyo networks to access the Internet for outside business interests.***

For additional information regarding Kinyo's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (Company url).

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong passphrases. For further information see the Acceptable Encryption Policy and the Password Policy. All remote users must use the company always provided VPN.

4.1.2 Authorized Users shall protect their logon and password, even from family members.

4.1.3 While using a Kinyo-owned computer remotely connect to Kinyo's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal network that are under their complete control or under the complete control of Authorized Users or Third Party.

4.1.4 Use of external resources to conduct Kinyo business must be approve in advance by I.T. and the appropriate business unit manager. External resources include 3rd party file storage (such as drobox), personally supplied devices (such as computers, flash drives, and wireless adapters), and 3rd party applications not installed by Kinyo I.T.

4.1.5 All hosts that are connected to Kinyo Production internal networks must have up to date antivirus. The domain controller handles this process for all devices connected to the domain. Any device other than server's setup by the I.T. department on Kinyo Production networks must have written approval of IT to be on the network and not connected to the domain. A domain account ends with @kinyova.com.

4.1.6 Personal equipment used to connect to Kinyo's production networks must meet the requirements of Kinyo-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to Kinyo Networks. Each personal device must have the written approval of I.T.

4.1.7 All equipment given to Kinyo Employees must be signed out using the "Kinyo Owned Equipment Form."

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, periodic walk-thru, video monitoring, business tool reports, internal and external and its, and inspections, and will provide feedback to the policy owner and appropriate business unit manager. The I.T. will block access to Kinyo Networks for any device not in the list of approved devices for security reasons.

5.2 Exceptions: Any exception to the policy must be approve by Remote Access Services and the I.T. department in advance.