## 1. Overview

I.T. Department intentions for publishing an Unacceptable Use Policy are not to impose restrictions that are contrary to the Kinyo established culture of openness, trust, and integrity. I.T. is committed to protecting Kinyo employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet, Intranet systems, including but not limited to computer equipment, login information, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are systems that Kinyo Employees uses are to be use for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resource policies for further details.

Effective security for these computer systems used for Kinyo is a team effort involving the participation and support of every Kinyo employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2. Purpose

The purpose of this policy is to outline the unacceptable use of computer equipment at Kinyo. These rules are in place to protect the employee and the Company from inappropriate use of computer equipment that exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. Scope

This policy is applied to the use of information, electronic equipment, computing devices, and network resources, whether owned or leased by Kinyo, to conduct Kinyo business by Kinyo Employees. It also applies to any personal device that stores or has ever stored Kinyo data. A personal device that previously stored Kinyo data can be cleared by the I.T. manager and released from this policy after it is confirmed to have no Kinyo data.

## 4. Policy

### 4.1 General Use and Ownership

4.1.1 Information stored on electronic and computing devices whether owned or leased by Kinyo (hereinafter called Kinyo Information) is the sole property of Kinyo. Kinyo Employees and anyone else with access to Kinyo data must ensure through legal or technical means Kinyo Information is protected in accordance with Data Protection Standard.

4.1.2 Kinyo Employees have a responsibility to promptly report to the I.T. Department any theft, loss, or unauthorized disclosure of Kinyo Information.

4.1.3 Kinyo Employees may access, use, or share Kinyo proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgement regarding personal use of any company resource. Individual departments are allowed to create guidelines concerning personal use of Internet/Intranet/Extranet systems if it does not violate this or any other Kinyo policy. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Kinyo may monitor equipment, systems, and network traffic at any time, per I.T. Department Audit Policy.

4.1.6 Kinyo reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy. All Kinyo owned devices, devices that access production networks, and personal devices with access to Kinyo data; must connect to the network using an I.T. provided domain account. Local accounts are prohibited without written permission from the I.T. department.

4.2.2 System level and user level passwords must comply with Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. Only the I.T. department gives access to internal networks.

4.2.3 All computing devices must be secure with a password-protected screensaver or lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Kinyo email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Kinyo, unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

4.3.1 The following activities are, in general, prohibited. Employees may be exempt from these restrictions during them legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Kinyo authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Kinyo-owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### 4.3.1 System and Network Activities

The following activities are prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Kinyo.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of or use of any copyrighted software for which Kinyo or the end user does not have an active license is prohibited.

3. Accessing data, a server, or an account for any purpose other than conducting Kinyo business, even if you have authorized access, is prohibited. Accessing any system using credentials other than credentials provided to you by Kinyo is prohibited.

4. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws, is illegal. The appropriate management should be consult prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being completed at home.

7. Using a Kinyo computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment laws or hostile workplace laws in the user’s local authority.

8. Making fraudulent offers of products, items, or services originating from any Kinyo account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions or network communication. Security breaches include, but are not limit to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorize to access, unless these duties are with the scope of regular duties. For purposes of this section, “disruption” includes, but is not limit to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security is expressly prohibited unless prior notification to I.T. department.

12. Executing any form of network monitoring which will intercept data not intended for the employee’s host unless this activity is a part of the employee’s normal job/duty.

13. Circumventing any user authentication or security on any host, network, or account.

14. Introducing honeypots, honeynets, or similar technology on the Kinyo network.

15. Interfering with or denying service to any user (for example, denial or service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Kinyo employees to parties outside Kinyo Virginia Inc.

### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, user must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be address to the I.T. Department.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email or telephone whether through language, frequency, or size of messages.

- Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding "chain letters," Ponzi or other "pyramid' schemes of any type.

- Use of unsolicited email originating from within Kinyo network of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Kinyo or connected via Kinyo network.

### 4.3.3 Blogging and social media

- Blogging by employees, whether using Kinyo property or systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Kinyo systems to engage in blogging is unacceptable, if it done in a professional and responsible manner, does not otherwise violate, Kinyo policy, is not determined to Kinyo best interests, and does not interfere with an employee's regular work duties. Blogging from Kinyo systems is also subject to monitoring.

- Kinyo Confidential Information policy also applies to blogging. As such, employees are prohibiting from revealing any Kinyo confidential or proprietary information, trade secrets or any other material covered by Kinyo Confidential Information policy when engaged in blogging.

- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Kinyo and/or of its employee. Employees are also prohibiting from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Kinyo Non-Discrimination and Anti-Harassment policy.

- Employees may also not attribute personal statements, opinions, or beliefs to Kinyo when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Kinyo. Employees assume all risk associated with blogging.

- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Kinyo trademarks, logos and any other Kinyo intellectual property may also not be use in connection with any blogging activity.

## 5. Policy Compliance

### 1.1 Compliance Measurement

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

### 1.2 Exceptions

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