Quality Document	**Kinyo Virginia, Inc.**			
Anti-Virus Policy			**Issue: ITP004**	
Date: 07/20/2022	Approved: F. Koshiji	Issued By: I.T. Department	Revision: 001	Page **1** of **3**

1. Purpose

1.1 One of the goals Kinyo Virginia, Inc. (KVI) is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by KVI employees to help achieve effective virus detection and prevention.

Definition – Virus; A virus is a piece of potentially malicious programming code that will cause unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, thumb drives, and CD's etc. Viruses usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to KVI in terms of lost data, lost staff productivity, and/or lost reputation.

2. Scope

2.1 This policy applies to all KVI computers that are PC-based or use PC-file directory sharing. This includes, but not limited to, desktop computers, file/ftp/tftp/proxy servers, and any PC-based equipment.

3. Policy

All KVI PC-based computers must have Kinyo's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be up to date. Kinyo's I.T. team has recommended the processes to ensure that anti-virus software run at regular intervals, and to keep computers virus-free.

3.1 Recommended processes to prevent virus problems:

3.1.0 Always run the standard anti-virus software provided by Kinyo Virginia, Inc.

3.1.1 Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3.1.2 Never open any files or macros attached to an e-mail from known source (even a coworker) if you were not expecting a specific attachment from that source.

3.1.3 Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

3.1.4 Files with the following filename extension are blocked by the e-mail system: [.exe, .bat etc.]. Business files with banned extension can be sent /received by compressing the same in a folder by use of a file compression utility.

3.1.5 Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

3.1.6 Avoid direct disk sharing with read/write access. Always scan any storage media for viruses before using it.

3.1.7 If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your deleted items or trash folder.

3.1.8 Back up critical data and systems configurations on a regular basis store backups in a safe place.

3.1.9 Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

3.1.10 Backup critical files and store the files in a safe place like “OneDrive or Sharepoint”.

Any activities with intention to create and/or distribute malicious programs into KVI’s networks (e.g., viruses, worms, trojan horses’ logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, please contact I.T. Department. Do not turn off your computer, it will be quarantined and taken off the network until it can be scanned and re-imagined with the operating system image.

3.2 I.T. Department Responsibilities

The following activities are the responsibility of Kinyo Virginia, Inc. I.T. department:

3.2.0 The I.T. department is responsible for maintain and updating this Anti-Virus Policy. Copies of this policy will be posted on our Kinyo sharepoint website under the I.T. Department shared folder. Check this location regularly for updated information.

3.2.1 The I.T. department will apply any updates to the services it provides that are required to defend against threats from viruses.

3.2.2 The I.T. department will install anti-virus software on all KVI’s desktops workstations, laptops, and servers.

3.2.3 The I.T. department will take appropriate action to contain, remove, and assist in recovery from virus infections. To do so, the I.T. department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

3.2.4 The I.T. department will perform regular anti-virus sweeps of Windows desktop OS and user files.

3.2.5 The I.T. department will attempt to notify users of KVI of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages to keep network traffic to a minimum.

3.2.6 If an employee is suspected of causing an incident, the I.T. department may need to notify human resource department for further review – for example, in assisting with disciplinary proceedings.

3.2.7 Employees should be aware and trained of policies and procedures regarding appropriate use of networks, systems, and applications.

3.3 Department and Individual Responsibilities

The following activities are the responsibility of KVI department and employees:

3.3.0 Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy.

3.3.1 Department that allows employees to use personally owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3.3.2 All employees are responsible for taking reasonable measures to protect against virus infection.

3.3.3 Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the KVI network without the express consent of the I.T. Department.

4. Policy Compliance

4.1 Compliance Measurement:

The I.T. Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the I.T. Department.

4.2 Exceptions:

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