1. Overview:

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. Removable Media must be controlled very closely and the need for removable storage must be reviewed frequently.

2. Purpose:

This policy is to minimize the risk of loss or exposure of sensitive information maintained by Kinyo and to reduce the risk of acquiring malware infections on computers operated by KVI employees.

3. Scope:

Is to cover all computers, servers, and removable media operating at Kinyo Virginia Inc. Removable media is any device capable of storing data that is not internal to your computer. Removable media is also any 3rd party hosting site not authorized by the Kinyo I.T. Manager. Sending files via email is considered removable media as the file is stored remotely. Any internal drive that is removed from inside a computer is removable media.

The AWS drives by I.T. Department is not considered removable media by this policy. The remote storage in Microsoft Teams managed by Kinyo I.T. Department is not considered removable media. The remote storage in Microsoft Sharepoint that is managed by I.T. is not considered removable media. The Microsoft OneDrive storage is not considered removable media when it is connected to your @kinyova.com domain account provided by I.T.

4. Policy

4.1 No Kinyo employee has access to removable media by default except the I.T. Department and the executive branch. Anyone else must request access from the I.T. department and this is subject to a review.

4.2 A Kinyo removeable media is a device that is bought, owned, maintained, and secured by Kinyo. Kinyo staff may only use Kinyo removable media in their own assigned work on computers. Kinyo removable media may not be connected to or used in computers that are owned or leased by the Kinyo without explicit permission of the Kinyo I.T. Manager. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Kinyo I.T. Department requirements.

4.3 No removable media may be connected to a Kinyo computer unless the removable media is a Kinyo removable media. No outside removable media should be brought into Kinyo unless approved by I.T. No Kinyo removable media should ever be attached to a device not owned by Kinyo.

4.4 Exceptions to this policy may be requested on a case-by-case basis Kinyo-exception procedures. Exceptions are approved by I.T. Department Manager in writing using the “Kinyo Removable Media Access form.”

5. Policy Compliance

5.1 Compliance Measurement

The I.T. department will verify compliance to this policy through various methods, including but not limited

to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. The I.T. team can collect any removable media on Kinyo property for inspection without reason.

5.2 Exception,

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