<table>
<tr><td colspan="2"><b>System Document</b></td><td colspan="3"><b>Kinyo Virginia Inc.</b></td></tr>
<tr><td colspan="4"><b>Software Installation Policy</b></td><td><b>Issue: ITP020</b></td></tr>
<tr><td>Date: 7/22/2022</td><td>Approved: F. Koshiji</td><td>Issued By: I.T. Department</td><td>Revision: 001</td><td>Page <b>1</b> of <b>1</b></td></tr>
</table>

1. Overview

Allowing employees to install software on company computer devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installations software, unlicensed software which could be discovered during an audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2. Purpose

The purpose of this policy is to outline the requirements around installation software on Kinyo computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Kinyo computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This policy applies to all KVI employees, contractors, vendors, and agents with a Kinyo-owned mobile devices. This policy covers all computers, servers, smartphones, tablets, and other computing devices operating within Kinyo.

4. Policy

4.1 Employees may not install software on Kinyo computing devices operated within the Kinyo network or working home.

4.2 Software request must be first approved by the department manager and then be made to the I.T. department via Kinyo osTicket support website.

4.3 Software must be selected from an approved software list, maintained by the I.T. department, unless no selection on the list meets the requestor's need.

4.4 The I.T. department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Policy Compliance

5.1 Compliance Measurement

The I.T. department team 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 I.T. department.

5.2 Exceptions

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