1. Purpose

This document describes a required minimal security configuration for all routers and switches connecting toa production network or used in a production capacity at or on behalf of Kinyo Virginia, Inc.

2. Scope

All employees, contractors, consultants, temporary and other workers at Kinyo and its subsidiaries must adhere to this policy.

3. Policy

Every router must meet the following configuration standards.

4.1 No local user accounts are configured on the router. Routers and switches must use all user authentications.

4.2 The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organizations.

3.3 The following services features must be disabled:

a. IP directed broadcasts
b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.
c. TCP (transmission control protocol) small services
d. UDP (user datagram protocol) small services
e. All source routing and switching
f. All web services running on router
g. Kinyo discovery protocol on internet connected interfaces
h. Telnet, FTP, and HTTP services
i. Auto-configurations

3.4 The following services should be disabled unless a business justification is provided:

a. Kinyo discovery protocol and other discovery protocols
b. Dynamic trunking protocol
c. Scripting environments, such as the TCL shell

4.5 The following services must be configured:

a. Password-encryption

b. NTP configured to a corporate standard source

4.6 All routing updates shall be done using secure routing updates.

4.7 Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

4.8 Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

4.9 Access control lists for transiting the device are to be added as business needs arise.

4.10 The router must be included in the management systems with a designated point of contact.

4.11 Each router must have the following statement presented for all forms of login whether remote or local:

"Unauthorized access to this network device is prohibited. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There s no right to privacy on this device. Use of this system shall constitute consent to monitoring".

4.12 Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communications path. SSH (secure shell protocol) is the preferred management protocol.

4.13 Dynamic routing protocols must be authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

4.14 The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

a. IP access list accounting
b. Device logging
c. Incoming packets at the router sourced with invalid addresses, or those that could be used to spoof network traffic shall be dropped.

d. Router console and modern access must be restricted by additional security controls.

4. Policy Compliance

5.1 Compliance Measurements

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 I.T. department.

5.2 Exceptions

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