System Document	**Kinyo Virginia, Inc.**			
Extranet Policy			**Issue: ITP010**	
Date: 05/26/2022	**Approved: F. Koshiji**	**Issued By: I.T. Department**	**Revision: 001**	***Page:*** 1 ***of*** 2

1. Purpose

1.1 This document describes the policy under which third party organizations connect to KVI (Kinyo Virginia, Inc.) networks for the purpose of transacting business related to Kinyo.

2. Scope

2.1 Connections between third parties that require access to non-public Kinyo resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology use for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide internet access for Kinyo or to the public switched telephone network DO NOT fall under this policy.

3. Policy

3.1 Pre-Requisites

3.1.1 Security Review

All new extranet connectivity will go through a security review with the I.T. department. The reviews are to ensure that all access matches the business requirements in a best feasible way, and that the principle of least access is followed.

3.1.2 Third Party Connection Agreement

All new connection requests between third parties and Kinyo require that the third party and Kinyo representatives agree to and sign the third-party agreement. The project manager must sign this agreement as well as a representative from the third party who is legal empowered to sign on behalf of the third party.

The signed document kept on file with the relevant extranet group. Documents pertaining to connections into Kinyo labs kept on file with the (name of team responsible for security of labs).

3.1.3 Business Care

All production extranet connections must be accompanied by a valid business justification, in writing, that is approve by a project manager in the extranet group. Lab connections must be approved by the (name of team responsible for security of labs). Typically, this function is managed as part of the third-party agreement.

3.1.4 Point of Contact

The project manager must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of and is responsible for those portions of this policy and the third-party agreement that pertain to it. If the point of contact changes, the relevant extranet organization must be informed promptly.

3.2 Establishing Connectivity

3.2.1 Any sponsoring organizations with Kinyo that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage Kinyo to address security issues inherent in the project.

3.2.2 If the proposed connections are to terminate within a lab at Kinyo, supervisor or upper management must engage the (name of team responsible for security of labs). Must also provide full and complete information as to the nature of the proposed access to the extranet group and Kinyo, as requested.

3.2.3 All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Kinyo relay upon the third party to protect Kinyo's network or resources.

3.3 Modifying or Changing Connectivity and Access

3.3.1 All changes in access must be accompanied by a valid business justification and are subject to security review. Changes are to be implement via corporate change management process. The project manager is responsible for notifying the extranet management group and/or Kinyo when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.4 Termination Access

3.4.1 When access is no longer require, the appropriate authorization within Kinyo must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.

3.4.2 The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still need, and that the access provided longer use to conduct Kinyo business, will be terminate immediately.

3.4.3 Should a security incident or a finding that a circuit has been deprecate and no longer used to conduct Kinyo business necessitate a modification of existing permissions, or termination of connectivity, Kinyo and/or the extranet team will notify the POC or the project manager of the change prior to taking any.

4. Policy Compliance

4.1 Compliance Measurement: The I.T. department 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.

4.2 Exceptions: Any exceptions to the policy approved by the I.T. department in advance.