

System Document		Kinyo Virginia, Inc.		
Communications Equipment Policy			Issue: ITP006	
Date: 7/22/2022	Approved: F. Koshiji	Issued By: I.T. Department	Revision: 001	Page: 1 of 2

1. Purpose:

This document describes requirements for communication equipment security configurations of Kinyo Virginia, Inc.

2. Scope:

This policy applies to all communication equipment that is part of the data network of and for Kinyo Virginia, Inc.

3. Policy

- 3.1 The security features necessary to minimize risks to communication equipment must be configured in the equipment before it is placed into service. There are two roles for the staff that manages the communication equipment: monitoring and administrator. The monitoring role has read only privileges. The administrator role can change configuration parameters. All issued commands by users will be recorded, as well as any other security events that may pose a threat to the equipment.
- 3.2 Local users are not allowed on communication equipment. Everyone must authenticate through the central repository of users using a protocol that reduces the risk of identity theft.
- 3.3 All information transmitted from the device must be encrypted to minimize the risks of eavesdropping on the communications and man-in-the-middle attacks.
- 3.4 The events recorded by the communication equipment must be kept in storage media that is subject to a regular backup process. The process of maintaining these backups must ensure that the information is not amended.
- 3.5 The password of the communication equipment's administrator user must not be known by anyone on the staff that manages the equipment. If, for any reason, it is necessary to make use of the highest administrative privileges within the device then the staff must file a request to the internal security division for the password attaching the justification for its use and completing the required forms. The highest administrator must then reset the password to maintain security.

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. team in advance.

System Document		Kinyo Virginia, Inc.		
Communications Equipment Policy			Issue: ITP006	
Date: 7/22/2022	Approved: F. Koshiji	Issued By: I.T. Department	Revision: 001	<i>Page: 2 of 2</i>