1. Purpose:

The purpose of this policy is to ensure all servers deployed at Kinyo are configured according to the Kinyo security policies. Servers deployed at Kinyo shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Ensure conformance to Kinyo security policies.

2. Scope

This policy covers all servers owned or operated by Kinyo. This policy also covers any server present on Kinyo premises and on the cloud, but which may not be owned or operated by Kinyo.

3. Policy

Kinyo hereby provides its consent to allow internal and external audit to access its servers to the extent necessary to allow audit organizations to perform scheduled and ad hoc audits of all servers at Kinyo.

4.1 Specific Concerns

Servers in use for Kinyo support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability, or integrity of these systems.

4.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include.

- All system logs shall be sent to a central log review system.
- All administrator actions must be logged.
- Use a central patch deployment system.
- Host security agent such as antivirus shall be installed and updated.
- Network scan to verify only required network ports and network shares are in use
- Verify administrative group membership
- Conduct baselines when systems are deployed and upon significant system changes.
- Changes to configurations template shall be coordinated with approval of change control board.

4.3 Responsibility

Internal and external audit shall conduct audits of all servers owned or operated by Kinyo. Server and application owners are encouraged to also perform this work as needed.

4.4 Relevant Findings

All relevant findings discovered because of the audit shall be listed in the Kinyo tracking system to ensure prompt resolution or appropriate mitigating controls.

4.5 Ownership of Audit Report

All results and findings generated by the internal or external audit team must be provided to appropriate Kinyo management within one week of project completion. This report will become the property of Kinyo and be considered company confidential.

4. Policy Compliance

4.1 Compliance Measurement

Internal and external audit name shall never use access required to perform server audits for any
other purposes.

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 policy owner.

5.2 Exceptions

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