1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent server installation policies, ownership and configuration management are all about doing the basic well.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Kinyo. Effective implementation of this policy will minimize unauthorized access to Kinyo propriety information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers, and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased, and or registered under the internal network domain.

This policy specifies requirements for equipment on the internal network. For secure configuration of equipment external on the DMZ, see the Internet DMZ Equipment Policy, (ITP011).

4. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at Kinyo must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the I.T. team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by I.T. team. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact (s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable.
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures.

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved I.T. team guidelines.

4.2.2 Services and applications should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.3 Access to services should be logged and/or protected through access-control methods such as web application firewall, if possible.

4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5 Trust relationships between systems are a security risks, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels., (e.g., encrypted network connections using SSH or IPsec).

4.2.8 Servers should be physically located in an access-controlled environment.

4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive system must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2 Security-related events will be reported to I.T. team, who will review logs and report incidents to I.T. Management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts.
- Anomalous occurrences that are not related to specific applications on the host.

5. Policy Compliance

5.1 Compliance Measurement

The I.T. 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 policy owner.

5.2 Exceptions

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