1. Purpose

1.1 The purpose of this policy is to define standards to be met by all equipment owned and/or operated by KVI internet firewalls. These standards are designed to minimize the potential exposure to KVI from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of KVI resources.

1.2 Devices that are internet facing and outside the KVI firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

2. Scope

2.1 All equipment or devices deployed in a DMZ owned and/or operated by KVI (including hosts, routers, switches, etc.) and/or registered in any domain name system (DNS) domain owned by KVI, must follow this policy. This policy also covers any host device outsourced or hosted at external/third-party service providers if that equipment resides in the "Kinyo Virginia Inc.com" domain or appears to be owned by KVI.

2.2 All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents unless a waiver is obtained from I.T. team. All existing and future equipment deployed on KVI's un-trusted networks must comply with this policy.

3. Policy

3.1 Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by I.T. team for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required.
    - Host contacts and locations
    - Hardware and operating system/version

- Main functions and applications
- Password group for privileged passwords

- Network interfaces must have appropriate Domain Name Server (DNS) records (minimum of A and PTR records).

- Password groups must be maintained in accordance with the corporate wide password management system/process.

- Immediate access to equipment and system logs must be granted to members of I.T. team upon demand, per the audit policy.

- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this policy, I.T. team will periodically audit DMZ equipment per the audit policy.

4.2 General Configuration Policy

4.2.1 All equipment must comply with the following configuration policy:

- Hardware, operating systems, services, and applications must be approved by I.T. team as part of the pre-deployment review phase.

- Operating system configuration must be done according to the secure host and router installation and configuration standards.

- All patches/hot fixes recommended by the equipment vendor and I.T. team must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.

- Services and application not serving business requirements must be disabled.

- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by I.T. team.

- Services and applications not for general access must be restricted by access control lists.

- Insecure services or protocols (as determined by I.T. team) must be replaced with more secure equivalents whenever such exists.

- Remote administrations must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords must be used for all access levels.

- All host content updates must occur over secure channels.

- Security-related events must be logged, and audit trails saved by I.T. team-approved logs.

- Security-related events include (but are not limited to) the following:

    - User login failures

    - Failure to obtain privileged access

    - Access policy violations

- I.T. team will address non-compliance waiver request on case-by-case basis and approved waivers if justified.

4.3 New Installation and Change Management Procedures

4.3.1 All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the DMZ equipment deployment process.

- Configuration changes must follow the Corporate Change Management (CM) Procedures.

- I.T. team must be invited to perform system/application audits prior to the deployment of new services.

- I.T. team must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

4.4 Equipment Outsourced to External Service Providers

4.4.1 The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting department are responsible for third-party compliance with this policy.

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, 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. team in advance.