Internet DMZ Equipment Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
The purpose of this policy is to define standards to be met by all equipment owned and/or operated by <Company Name> located outside <Company Name>'s corporate Internet firewalls. These standards are designed to minimize the potential exposure to <Company Name> from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of <Company Name> resources.

Devices that are Internet facing and outside the <Company Name> 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

2.0 Scope
All equipment or devices deployed in a DMZ owned and/or operated by <Company Name> (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by <Company Name>, 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 "<Company Name>.com" domain or appears to be owned by <Company Name>.

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 InfoSec. All existing and future equipment deployed on <Company Name>'s un-trusted networks must comply with this policy.

3.0 Policy

3.1. Ownership and Responsibilities
Equipment and applications within the scope of this policy must be administered by support groups approved by InfoSec 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 location.
    - Hardware and operating system/version.
    - Main functions and applications.

    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server 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 InfoSec 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, InfoSec will periodically audit DMZ equipment per the *Audit Policy*.

3.2. General Configuration Policy
All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by InfoSec 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 [Insert a reference to any standards that you have]
- All patches/hot-fixes recommended by the equipment vendor and InfoSec 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/hotfixes.
- Services and applications 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 InfoSec.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by InfoSec) must be replaced with more secure equivalents whenever such exist.
- Remote administration 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 (DES/SofToken) 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 to InfoSec-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.3. New Installations and Change Management Procedures
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.
- InfoSec must be invited to perform system/application audits prior to the deployment of new services.
- InfoSec must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Equipment Outsourced to External Service Providers

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 departments are responsible for third party compliance with this policy.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
DMZ (de-militarized zone)	Any un-trusted network connected to, but separated from, <Company Name>'s corporate network by a firewall, used for external (Internet/partner, etc.) access from within <Company Name>, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.
Secure Channel	Out-of-band console management or channels using strong encryption according to the *Acceptable Encryption Policy*. Non-encrypted channels must use strong user authentication (one-time passwords).
Un-Trusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

6.0 Revision History