Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Internet DMZ Equipment*

Policy Purpose:

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

Devices that are Internet facing and outside the **Saratoga Bridges** firewall are considered part of the "demilitarized 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

All equipment or devices deployed in a DMZ owned and/or operated by **Saratoga Bridges**(including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by **Saratoga Bridges** 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 "**SaratogaBridges**.org" domain or appears to be owned by **Saratoga Bridges**.

All new equipment that falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from the IT Department. All existing and future equipment deployed on **Saratoga Bridges**'s un-trusted networks must comply with this policy.

Policy Description / Responsibilities:

Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by the IT Department 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 the IT Department upon demand.
- Changes to existing equipment and deployment of new equipment must follow any corporate governance or change management processes/procedures.

To verify compliance with this policy, the IT Department will periodically audit DMZ equipment.

General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services, and applications must be approved by the IT Department 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 the IT Department 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 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 the IT Department.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by the IT Department) 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 IT Department - approved logs. Security related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- The IT Department will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

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:

- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- The IT Department must be invited to perform system/application audits prior to the deployment of new services.
- The IT Department must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

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.

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