**Patch Management Policy**

**Overview:**

[Insert Covered Entity or Business Associate name] is responsible for ensuring the confidentiality, integrity, and availability of all Protected Health Information (PHI) stored on its systems. [Insert Covered Entity or Business Associate name] has an obligation to provide appropriate protection against threats, which could adversely affect the security of the system or its data entrusted on the system. Implementation of this policy will limit the exposure and possible effects of common malware threats to the systems.

**Purpose:**

To outline the requirements for maintaining up-to-date operating system security patches on all [Insert Covered Entity or Business Associate name] owned and managed workstations and servers.

**Scope:**

This policy applies to workstations or servers owned or managed by [Insert Covered Entity or Business Associate name]. The following systems have been categorized according to management (optional based on requirements of the organization):

1. Unix/Solaris servers managed by Unix Engineering Team
2. Microsoft Windows servers managed by Windows Engineering Team
3. Workstations (desktops and laptops) managed by Workstation Imaging Team

**Definitions**

1. Device: an object used to store, process, and/or transfer data.
2. Operating System (OS): the set of programs used to provide the basic functions of a computer.
3. Patch: A piece of software designed to fix problems or update a computer program or its supporting data.
4. Protected Health Information (PHI): Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. PHI does not include individually identifiable health information in education records covered and protected by the Family Educational Right and Privacy Act and employment records held by a covered entity in its role as an employer.
5. Trojan: A class of computer threats that appears to perform a desirable function, but in fact, performs undisclosed malicious functions.
6. Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
7. Worm: A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

**Policy**

1. Workstations and Servers
	1. Workstations and servers owned by [Insert Covered Entity or Business Associate name] must have up-to-date operating systems. This may require the installation of security patches to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by [Insert Covered Entity or Business Associate name].
	2. Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by [Insert Covered Entity or Business Associate name]. Any exception to the policy must be documented and forwarded to the Security Officer for review.
	3. Servers must comply with the minimum baseline requirements that have been approved by the Security Officer. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the [Insert Covered Entity or Business Associate name] asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the Security Officer for review.
2. Roles and Responsibilities (optional depending upon organizational requirements)
	1. Unix Engineeringwill manage the patching needs for the Linux, Unix, and Solaris servers on the network.
	2. Windows Engineeringwill manage the patching needs for the Microsoft Windows servers on the network**.**
	3. Workstation Imagingwill manage the patching needs of all workstations on the network.
	4. Information Securityis responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
	5. The Change Management Boardis responsible for approving the monthly and emergency patch management deployment requests.
3. Monitoring and Reporting
	1. Active patching teams noted in the Roles and Responsibility section are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to the Security Officer upon request.
4. Exceptions
	1. Exceptions to the patch management policy require formal documented approval from the [Insert Covered Entity or Business Associate name]. Any servers or workstations that do not comply with policy must have an approved exception on file with the [Insert Covered Entity or Business Associate name].
	2. Please refer to the Security Officer for details on filing exceptions.
5. Implementation and Enforcement
	1. The Security Officer will implement this policy. Enforcement of this policy is ultimately the responsibility of all employees at [Insert Covered Entity or Business Associate name]. The Security Officer may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action.

**Violations:**

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Violations shall be noted in the [Insert Covered Entity or Business Associate name] issue tracking system and support teams shall be dispatched to remediate the issue.