**Patch Management Policy**

**Overview:**

Trialomics, Inc is responsible for ensuring the confidentiality, integrity, and availability of all Protected Health Information (PHI) stored on its systems. Trialomics, Inc 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 Trialomics, Inc owned and managed workstations and servers.

**Scope:**

This policy applies to workstations or servers owned or managed by Trialomics, Inc. The following systems have been categorized according to management:

1. EC2 servers running Picard API
2. Workstations used by users who can access systems with ePHI.

**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 Trialomics, Inc must have reasonably 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 Trialomics, Inc.
   2. Servers must comply with the minimum baseline requirements that have been approved by the Information 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 Trialomics, Inc asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the Information Security Officer for review.
2. Roles and Responsibilities
   1. The Information Security Officerwill manage the patching needs for the Linux, Unix, and Solaris servers on the network.
   2. Workstation management is the responsibility of the employee.
   3. The Information Security Officeris responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
3. Monitoring and Reporting
   1. Patches to EC2 servers, including updates to the Picard API, will be saved and implemented as Amazon AMIs.This allows the Information Security Officer to determine requirements for current and previously used systems as needed.
4. Implementation and Enforcement
   1. The Information Security Officer will implement this policy. Enforcement of this policy is ultimately the responsibility of all employees at Trialomics, Inc. 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.