Patch Management 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 Overview
<Company Name> is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. <Company Name> has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

2.0 Purpose
This document describes the Global Security Office's (GSO) requirements for maintaining up-to-date operating system security patches on all <Company Name> owned and managed workstations and servers.

3.0 Scope
This policy applies to workstations or servers owned or managed by <Company Name>. This includes systems that contain company or customer data owned or managed by <Company Name> regardless of location. The following systems have been categorized according to management:

- Unix/Solaris servers managed by Unix Engineering Team
- Microsoft Windows servers managed by Windows Engineering Team
- Workstations (desktops and laptops) managed by Workstation Imaging Team

4.0 Policy
Workstations and servers owned by <Company Name> must have up-to-date (as defined by GSO's minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by <Company Name>.

4.1 Workstations
Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by <Company Name>. Any exception to the policy must be documented and forwarded to the GSO for review. *See Section 8.0 on Exceptions.*

4.2 Servers
Servers must comply with the minimum baseline requirements that have been approved by the GSO. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the <Company Name> asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the GSO for review. *See Section 8.0 on Exceptions.*

5.0 Roles and Responsibilities

- **Unix Engineering** will manage the patching needs for the Linux, Unix, and Solaris servers on the network.

- **Windows Engineering** will manage the patching needs for the Microsoft Windows servers on the network**.**

- **Workstation Imaging** will manage the patching needs of all workstations on the network.

- **Information Security** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

- **The Change Management Board** is responsible for approving the monthly and emergency patch management deployment requests.

6.0 Monitoring and Reporting
Active patching teams noted in the Roles and Responsibility section (5.0) 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 Information Security and Internal Audit upon request.

7.0 Enforcement
Implementation and enforcement of this policy is ultimately the responsibility of all employees at <Company Name>. Information Security and Internal Audit 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 shall be noted in the <Company Name> issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

8.0 Exceptions
Exceptions to the patch management policy require formal documented approval from the GSO. Any servers or workstations that do not comply with policy must have an approved exception on file with the GSO. *Please refer to the GSO or local Information Security representative for details on filing exceptions.*

7.0 Definitions

Term	**Definition**
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

6.0 Revision History
1.0 initial policy version, 4/28/2009