Insert Company Name and Logo	
Title: Software Patch Management	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy outlines the requirements for maintaining up-to-date operating system security patches on all [Insert Company name] owned and managed workstations and servers. Implementation of this policy will limit the exposure and possible effects of common malware threats to the systems.

Scope: This policy applies to workstations, servers or storage devices owned or managed by [Insert Company 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. Operating System (OS): the set of programs used to provide the basic functions of a computer.
2. Patch: A piece of software designed to fix problems or update a computer program or its supporting data.
3. Sensitive and Regulated Data: Data that includes information regulated by governing agencies, such as Protected Health information (PHI.)
4. Trojan: A class of computer threats that appears to perform a desirable function, but in fact, performs undisclosed malicious functions.
5. Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
6. Worm: A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Procedure:

1. Workstations and Servers

    a. Workstations and servers owned by [Insert Company 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 other workstations and servers. Where operations make currency of operating systems and other software patches impossible, the Security Officer must approve and document the approved state of the system. Each such system must be isolated as completely as possible from other devices and communications on the network. These devices shall also receive additional monitoring to ensure that the insufficiently patched systems do not fall victim to a cybersecurity event, incident, or attack.

    b. Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by [Insert Company name]. Any exception to the policy must be documented and forwarded to the Security Officer for review and other protections put in place as noted in (a).

    c. 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 Company 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 and other protections put in place as noted in (a).

2. Roles and Responsibilities (optional depending upon organizational requirements)

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

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

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

    d. 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.

    e. The Security Officer and/or Change Management Board/Committee is responsible for approving the monthly and emergency patch management deployment requests.

3. Monitoring and Reporting

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. 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. Risk Ranking

The organization uses the National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS), to determine risk ranking for security-related software patches, updates, and fixes. Issues with a CVE ranking can be found here: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&search_type=all&isCpeNameSearch=false

CVSS assigns the following qualitative severity rankings to vulnerabilities associated with security-related patches:

1. Low (CVSS 0.0-3.9)
1. Medium (CVSS 4.0-6.9)
1. High (CVSS 7.0-10.0)

Security patches self-designated as the highest level of criticality by a vendor must be treated as a **high** risk regardless of the CVSS score if the patch applies to any of the company's system components.

5. Security Patching Schedule

	Workstation Class Systems (e.g., Desktops, Laptops)	Other Sensitive Data Environment or Connected Systems (Servers, Networking / Security Devices)	Non-sensitive Data Environments
Available High/Medium security patches must be applied to system components	Prior to initial installation into the production environment.	Prior to initial installation into the production environment.	Prior to initial installation into the production environment.
High security patches must be applied	Within 30 calendar days of the vendor's release date.	Within 30 calendar days of the vendor's release date.	Within 30 calendar days of the vendor's release date.
Medium security patches must be applied	Within 30 calendar days of the vendor's release date.	Within 90 calendar days of the vendor's release date.	Within 180 calendar days of the vendor's release date.
Low security patches must be applied	Within 90 calendar days of the vendor's release date.	Within 365 calendar days of the vendor's release date.	Within 365 calendar days of the vendor's release date.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

6. Exceptions

    a. Exceptions to the patch management policy require formal documented approval from the Security Officer. Any servers or workstations that do not comply with policy must have an approved exception on file with the Security Officer.

    b. Please refer to the Security Officer for details on filing exceptions.

7. Implementation and Enforcement

    The Security Officer will implement this policy. Enforcement of this policy is ultimately the responsibility of all employees at [Insert Company 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.

8. Rollback Process

    When applying patches to critical and sensitive information system components, system administrators should create rollback procedures as appropriate.

Violations: Consequences for non-compliance may include, but not be limited to, device quarantine, disconnection from the network, or denial of access to or from applications or services.

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 Company name] issue tracking system, and support teams shall be dispatched to remediate the issue.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.