CONE HEALTH	**Guideline:** ITS Patch Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
System administrators

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with patch management.

Scope and Goals:
This procedure describes the organization's approach to patch management to include roles and responsibilities. While the primary focus of patch management is security related, this procedure is meant to focus on all types of patch management. Patch management includes all information technology assets: workstations, laptops, servers, network and security devices, personal devices, etc. The goals of this procedure are as follows:

- Define a process for review and framework for assigning priority.
- Assign responsibility for how patches are to be tested and implemented.
- Assign responsibility for patching personally owned devices used in the workplace.
- Provide guidance for identifying, evaluating, implementing, and testing security patches, to include prioritization.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to, the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Periodically assessing the adequacy of patch management processes.
- Ensure workforce members are periodically reminded that they are responsible for ensuring their personal devices are up to date on security patches, if they use their personal device for work related duties.

Information and Technology Services (ITS):
ITS is responsible for, but not limited to, the following activities:

- Maintaining patch management technology.
- Subscribing to and periodically researching/scanning reliable resources to proactively identify vulnerabilities and associated patches.

- Evaluating the criticality of patches and assess applicability.
- Ensuring patches are applied to all production and disaster recovery environments in a timely manner.
- Ensuring critical systems are not set to automatically patch/update.
- Change management process as it applies to the testing, rollback (if necessary) and deployment of any patches. Refer to the Change Management procedure.

Third-Party Vendors:

Vendors who are contractually responsible to maintain information technology assets, systems and applications on behalf of Cone Health will be responsible for their own patch management provided:

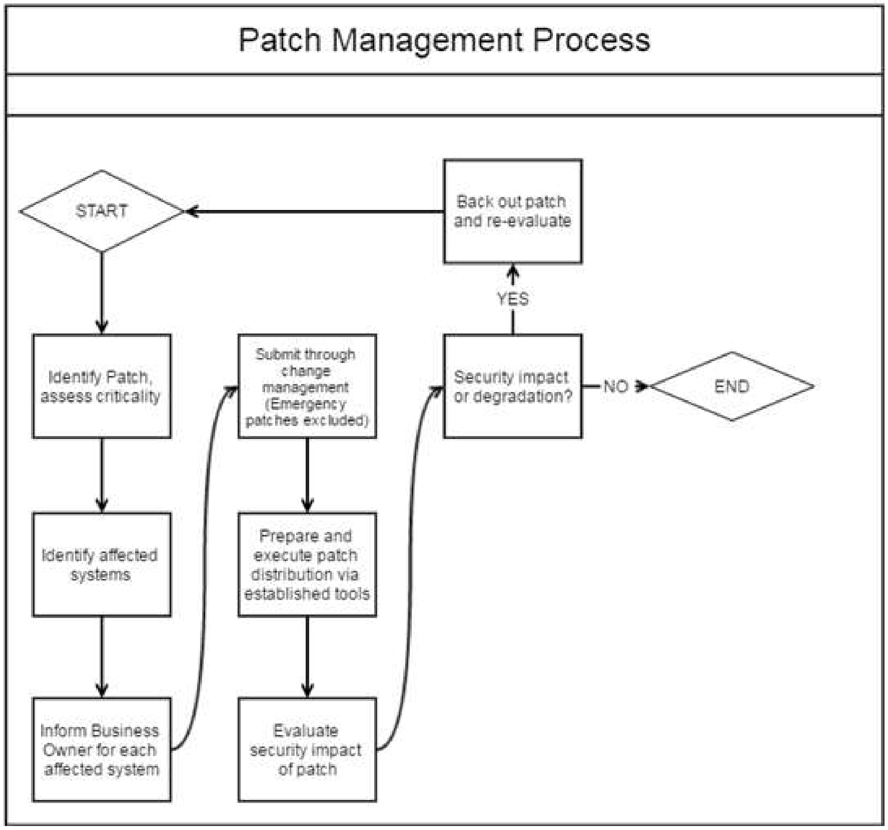
- It does not violate requirements outlined in this procedure.
- Patch deployment will be pre-coordinated and approved by ITS and if necessary, included in Cone Health’s change management process.

Workforce:

Workforce members who have been approved to use personal devices in the workplace for work-related duties are responsible for ensuring their device is always up to date on patches that are related to security vulnerabilities.

Patch Management Process:

Due to the risk associated to security patches, timely processing is absolutely critical to ensure that the representative risk posed by the vulnerability is mitigated. Consequently, it is recommended that security related patches be treated as any other production problem. The following is a high-level workflow for the patch management process.


Patch Management Process
START
Back out patch and re-evaluate
YES
Identify Patch, assess criticality
Submit through change management (Emergency patches excluded)
Security impact or degradation?
NO
END
Identify affected systems
Prepare and execute patch distribution via established tools
Inform Business Owner for each affected system
Evaluate security impact of patch

Patch Verification:
Cone Health ITS will only utilize trusted sources for system/application patches.

Evaluation of Patch Criticality:
Patches have varying criticality levels. Some patches are for difficult-to-exploit vulnerabilities, while others protect against rapidly spreading viruses. When a security bulletin is received with information on a newly released patch, Cone Health ITS will evaluate the criticality of the patch to ensure that the proper course of action is taken, taking the following under consideration:

- How will the patch affect the system (e.g., understanding what services and/or ports will be disabled, and what other changes may occur).
- What is the business impact if the patch is deployed?
- What is the risk to the business if deployed of the patch is delayed?
- What is the approximate size of the patch?

Patch Criteria	Criticality
Immediate patching is necessary to ensure the security of the individual system, and the overall security of Cone Health systems. - Systems or applications affected are business critical, and - Exploit is likely or possible, and - No workaround exists, and - Exploit could potentially compromise additional Cone Health systems, and - Exploit could potentially compromise Cone Health member information, or - Is exposed outside of other perimeter defenses.	Critical
Urgent patching is necessary to ensure the security of the individual system, and the overall security of Cone Health systems. - Systems or applications affected are business critical, and - Exploit is likely or possible, and - No workaround exists, and - Exploit could potentially compromise additional Cone Health systems.	Important
Action is required soon, although it may be postponed due to business need. - Systems or applications affected are non-business critical, and - Exploit is likely or Exploit is possible, but more difficult to implement, and - No workaround exists or Undesirable, but possible, workarounds exist.	Moderate
Action may be required, but thorough testing should be done before installation on production servers. - Systems or applications affected are non-business critical, and - Exploit is likely or Exploit is possible, but more difficult to implement, and - Viable workarounds exist.	Low

Note: Response time is directly related to the criticality of the system, business impact if the system goes down, likelihood the vulnerability could occur if the system remains unpatched and the sensitivity of the data residing on or passing through the information technology asset.

Based upon these definitions, specific Cone Health assets will be held to the following standards for time to the completion of remediation [patches applied across all affected systems]:

Deployment Timetable				
	Critical	Important	Moderate	Low
Servers in DMZ	Less than 24 hours	Less than 3 days	Less than 2 weeks	Patch included in the next scheduled maintenance cycle
Internal Servers	Less than 3 days	Less than 1 week	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle
Workstations	Less than 1 week	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle
Network devices - perimeter defense	Less than 24 hours	Less than 3 days	Less than 2 weeks	Patch included in the next scheduled maintenance cycle
Network devices - Internal	Less than 1 week	Less than 2 weeks	Patch included in the next scheduled maintenance cycle	Patch included in the next scheduled maintenance cycle

Pre-Deployment Testing:
ITS will test patches in a non-production environment that is as similar to the production environment. Testing is done for usability, security, and effects on other systems. The results of testing will then be documented and be included in the change control request and notification to business owners.

In the event a patch is found to be faulty, or the updated code is found to conflict with other software, ITS will remediate the conflict as soon as possible to avoid the risk of the affected system/application being vulnerable to a threat that the patch is meant to prevent.

Business Owner Notification:
Once ITS has evaluated the patch, determined deployment timeframe and completed a change control request, the appropriate business owners will be notified. Message details will include:

- The impact the patch has (or may have) on the affected system/application.
- Date/time the patch will be deployed.
- Provide a means for business owners to voice concerns.
- Reason for the patch and the risk of not implementing it.

Documentation Retention:
All patch management documentation related to testing, change management approval and deployment will be retained by ITS for a period of no less than 6 months.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.