CHS Community Health Systems

# Patch Management Standard

| | | | |
|---|---|---|---|
| **Sponsor:** | VP of Information Systems | **Area:** | Information Systems |
| **Effective Date:** | | **Description:** | Patch Management Standard |
| **Next Review Date:** | | **Policy Number:** | IS-STD-005 |
| **Supersedes:** | 1.0 (2009/05/14) | **Page:** | 1 of 5 |

## Purpose:

CHS's computers must be properly patched with the latest appropriate updates in order to reduce system vulnerability and protect the entire network from malicious attack. The purpose of this document is to establish the standard for the safe and timely installation of patches. These measures help to maintain the integrity, stability and reliability of the production IT environment, minimize service disruptions to the computing environment, and promote system availability.

## Scope:

This policy applies to all aspects of the CHS computing infrastructure, including servers, desktops, laptops, system software, applications, and network devices (routers, switches, etc.).

## Policy:

One of the largest threats to data security in any computing environment is the presence of outdated software with known vulnerabilities. Thus, it is critically important that patches are kept up-to-date on network devices, PCs, and servers on the CHS network.

### New Patch Assessment

The first step in the patching process is to evaluate the patches that have been released since the previous patching cycle. If the patch is not applicable, or if research determines that it may cause a problem, CHS may choose not to deploy the patch or to delay deployment while the patch is tested.

CHS uses MS System Center to scan its systems for security vulnerabilities. CHS' systems are scanned for vulnerabilities with the following frequency:

- Servers scan and update MS System Center every 4 hours.
- Desktops scan and update the MS System Center every 15 to 20 minutes.
- Laptops scan and update the MS System Center every 15 to 20 minutes.

Microsoft has issued severity ratings for patches to its products, due to the exploitability of known issues with the programming code. Rankings of 1 (critical) to 4 (low) are assigned as follows:

1. Critical - Exploitation could allow the propagation of an Internet worm such as Code Red or Nimda without user action.
2. Important - Exploitation could result in compromising the confidentiality, integrity, or availability of users' data or in the integrity or availability of processing resources.
3. Moderate - Serious vulnerability, but exploitability mitigated to a significant degree by factors such as default configuration, auditing, need for user action, or difficulty of exploitation.
4. Low - Exploitation is extremely difficult, or impact is minimal.

Each vulnerability alert must be checked against existing CHS systems and services prior to taking any action in order to avoid unnecessary patching. Read all alerts very carefully – not all patches are related to vulnerability issues or actual system versions present at CHS.
The following matrix represents CHS' methodology for determining timeframes (i.e., urgency) for patch deployment. This is derived by using the number of CHS systems/devices that require the patch plus the

severity level  Microsoft has given the vulnerability (described above). From those, we derived the CHS Threat Rating:

| CHS Threat Rating | Percentage of Environment Affected | Impact (Microsoft Severity Rating Scale) | | | |
|---|---|---|---|---|---|
| | | Low | Moderate | Important | Critical |
| Low | 0-15% | Low | Moderate | Moderate | High |
| Moderate | 16-39% | Low | Moderate | High | High |
| High | 40-74% | Moderate | Moderate | High | Critical |
| Very High | 75-100% | Moderate | High | High | Critical |

**Patching Schedule**

The timeframe (i.e., schedule) for patch deployment shall follow the guidelines presented in the deployment time table below.

| CHS Threat Rating | SLA Workstations | SLA Servers |
|---|---|---|
| Very High | 12  Hours | 48 Hours |
| High | 14 Days | 19 Days |
| Moderate | 60 Days | 60 Days |
| Low | Quarterly or Next Service Pack Release | Quarterly or Next Service Pack Release |

Depending on circumstances, there may be reasons to accelerate deployment (e.g., a known issue has already arisen within the CHS network).  This is determined by the Patch Management Team in conjunction with the Corporate Security Officer.

Multiple patches may be applied by bundling the patches together and deploying them on the schedule commensurate with the most severe patch.  Example: two patches are released, one with a CHS Threat Rating of “Moderate,” one with a “High” rating. Both patches shall be rolled out based on the schedule for a high threat rating.

**Patch Sources**

The following information sources will be taken as primary authorities on existing and new system vulnerabilities. These sources shall be monitored by assigned IT personnel on an ongoing basis.

- Microsoft Security Notification Service.
- CA Security Advisor
- Technical Alerts – us-CERT.gov
- Vendor Notification

All patches must be downloaded from the relevant system vendor or other trusted source. Each patch’s source must be authenticated and the integrity of the patch verified and documented. All patches must be submitted to an anti-virus scan upon download.

**Deployment into TEST Environment**
Once patches have been approved for testing, they shall be deployed into a test (non-production) environment. This is so that the system(s) can be rebooted, unforeseen side effects evaluated, and operational stability verified without impacting patient care and/or production systems. If issues arise, workarounds are sought, tested, and documented prior to deployment in a production environment. All patches must be tested prior to full implementation since patches may have unforeseen side effects.

*Exceptions:*

- In rare cases, when the benefits outweigh the risks – such as an extremely critical patch for a vulnerability that has already been exploited on the CHS network – the deployment into a test environment may be skipped, and the patch may be deployed directly into the production environment in order to mitigate further damage to the CHS network due to the vulnerability.
- In some cases, a test environment may not be available. Such as may be the case when expensive network equipment requires patching, an EPROM update, or flash memory upgrade, for example. If no test environment is available, or if the criticality of the patch requires accelerated deployment, an intitial, limited deployment is recommended (e.g., patch only a single device or a "pilot group" and monitor it) before rolling out the patch to all similar devices/systems. CHS uses SCCM Console to aid in deploying patches to a pilot group.

Following deployment of patches into the TEST environment, the devices, applications and systems are monitored to determine whether the patches cause any problems. In the rare case that a patch had to be deployed into the production environment without testing, the Service Desk will monitor calls to the Service Desk which may be related to the systems(s) or device(s) patched. These issues would be reviewed in an expedited manner by the team performing the patching before approving the test patches for wider release. The period of testing and monitoring should be completed as swiftly as possible to avoid undue delay in applying the patch to the production environment.

Patches that were successfully deployed and tested in the TEST environment (or limited production environment) are approved by the CHS patch committee. For release to the wider production environment. All Service Desk tickets related to patching issues must have been reviewed before approving the test patches for production release.

**Deployment into Production**
Once patches have been approved for the production environment, they are scheduled to be deployed using the existing Change Management procedures. Because rebooting or IPL (Initial Program Load) of systems is often involved – necessitating some temporary downtime – these deployments must be scheduled and widely publicisized to users in advance, *and* the timing of deployment should coincide with non-peak use of the affected system(s), application(s) or device(s).

After the device patch has been implemented in production, network administrators, the patch team, and the Service Desk personnel all continue to monitor the environment. Calls to the Service Desk are related to patching shall be accelerated.

**Administration:**

- Vulnerability assessment and system patching shall only be performed by the Patch Administrator, Service Desk Manager, Security Manager, Change Management, and/or their delegates.
- All server, desktop, and laptop systems, including all hardware and software components, must be accurately listed in the IT Department asset inventory to aid in patching efforts. Once patches have been applied, all configuration and inventory documentation must be immediately updated in order to reflect the applied patches.
- New servers and desktops must be fully patched and hardened before coming online in order to limit the introduction of risk.
- A back-out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in a production environment the event that the patch has unforeseen effects.

**Audits:**
Audits shall be performed to ensure that patches have been applied as required and are functioning as expected.

## Definitions:

**Patch** – a piece of software which, when applied to existing software, improves its function, plugs vulnerabilities, or prevents malicious code from infiltrating the software.
**Network Devices** – this includes but is not limited to infrastructure components such as routers, switches, firewalls, filters, monitors, and load balancers.
**System Software** – this includes but is not limited to Microsoft Windows operating systems and applications deployed corporate-wide, such as MS-SQL Server, MS-Office, anti-virus, and others.
**Application Software** – this includes clinical and financial applications from HMS, McKesson, and others.

## Discipline:

Failure to comply with this policy may lead to disciplinary action up to and including termination.

## References:

HIPAA Security Act 164.308(a)(1) – Risk Assessment & Risk Management
HIPAA Security Act 164.308(a)(5)(ii)(B) – Protection from Malicious Software
CHS Change Management Policies & Procedures
CMS Security Standards: Configuration Management (CM)
NIST Publications: SP800-83

## REVISION HISTORY:

| | | | |
|---|---|---|---|
| | | | |
| | | | |