



**Workstation Changes/
Patch Deployment**

March 2, 2009

Procedure Basis: [UNMC Policy 6051: Computer Use and Electronic Information Security Policy](#)

PURPOSE

In order to ensure a secure environment, software patches and workstation changes will be deployed as soon as technically feasible. Appropriate testing and communication will be an integral part of the patch/upgrade deployment process.

DEFINITION:

Critical Vulnerabilities: Qualys (Vulnerability scanning vendor) category 4 or 5

Clinical Workstations: Workstations which are utilized to provide direct patient care.

Workstation Changes: For purposes of this document, workstation changes would include those items which require workstation personnel intervention (i.e. Centricity Enterprise client)

POLICY

UNMC ITS shall form a Patch/Workstation Change Management Committee comprised of the following area:

- Manager of ITS Customer Support Services, chair
- Members from ITS Workstation Support
- Members from ITS Helpdesk (as needed)
- System Administrators (as needed)
- ITS Associate Director for Operations & Customer Support Services (direction, guidance, and oversight)
- ITS Information Security Officer
- Other members from ITS (as needed)

The UNMC ITS Patch/Workstation Change Management Committee will be responsible for utilizing the tools available to determine which patches/changes should be installed and the timetable for installing patches/changes. The tools include, but are not limited to Qualys reports, vendor information, and information security listserv's.

The Patch/Workstation Change Management Committee shall evaluate the risk and determine the most appropriate mitigation strategy to the upgrade, vulnerability, or threat. Patch/upgrade deployments shall follow the timelines identified in Exhibit 1.

All Qualys identified critical vulnerabilities shall be evaluated for mitigation. If the vulnerabilities cannot be mitigated an exception form shall be submitted to the Information Security Officer (Exhibit 2)

PROCEDURE

1. The Manager of ITS Customer Support Services (or designee) shall develop a proposed list of patches/changes to be applied based upon the tools available.
 - a. NOTE: It shall be the responsibility of the manager of Customer Support Services to communicate workstation changes which affect the healthcare partners in a timely manner such that the healthcare partners can adequately test the changes within their environment. A minimum of two weeks will be needed to test and deploy changes.
2. The Patch/Workstation Upgrade Management Committee will review the proposal and approve the prioritization of the patch.
3. The Patch/Workstation Upgrade Management Committee will determine the testing time.
4. The Manager of ITS Customer Support Services (or designee) will submit a change request via the Change Management Process. Upon approval from the Change Advisory Board, the patch will be deployed to a test group of computers which represent the major risk areas of the organization.
5. The testing group will be responsible for (1) verifying that the patch does not impact business services and (2) the reporting of those results to the Manager of ITS Customer Support (or designee).
6. Upon successful testing of the patch, the Manager of ITS Customer Support Services (or designee) will submit a change request via the Change Management Process for production implementation of the patch.
 - a. NOTE: Updates/patches to *clinical workstations* will be scheduled for the first and third Tue/Wed/Thu of each month. No other changes will be implemented UNLESS an emergency change is identified. Late changes will follow the late change process as defined in Change Management.

EMERGENCY PROCESS

If an unscheduled patch is recommended by industry leaders to be applied as soon as possible, the Patch/Upgrade Management Committee will review information and formulate recommendation to management. A Patch may be implemented before data is entered in the change management tool or written approval is attained.

STAFF ACCOUNTABILITY

- UNMC Asst Vice Chancellor, Information Technology

Exhibit 1

Workstation Patch/Changes Deployment Time Frames

Priority	Definition	Recommended Time Frame	Maximum Recommended Time Frame
Emergency	Represents immediate risk to organization	Immediately	Immediately
Critical	Vendor defined	Within 24 hours	Within 2 weeks
High	Vendor defined	Within 1 month	Within 2 months
Medium	Vendor defined	Depending on availability, deploy a new service pack within 4 months	Employ the software update within 6 months
Low	Vendor defined	Depending upon features of patch, deploy within 1 year	Choose not to deploy at all.

Exhibit 2

Patch Deployment-Workstations

Request to Not Fix Category 4 or 5 vulnerability

Date: _____

Review Date: _____

Requestor: _____

QID: _____

Technical Description of Vulnerability:

Attach Qualys Case Documentation

Risk Mitigation Applied instead of applying fix:

Approvals: (Note email authorization will be accepted as signature)

Manager, ITS Customer Support

Date

Information Security Officer

Date

As appropriate:

UNMC Asst Vice Chancellor,
Information Technology Services

Date