SUNY DOWNSTATE Medical Center

# COMPUTER PATCH MANAGEMENT POLICY

**Policy #: DCC06A**



**Prepared by: Joel Stern**
**Associate Director – Network Services**

**Reviewed by: Brian Dennis Gaon**
**Information Security Officer**

**Reviewed by: Bert Robles,**
**Chief Information Officer**

**Approved by:**

**Co-Chair Enterprise It Steering Committee**

**Original Issue date:** 03/06

**Supersedes:** _____

**Approval Date:** 3/2/2006

**Distribution:**

☒ Administrative Manual
☒ Department Manual
☒ Patient Care Manual
☒ AOD Manual

**Issued by: Information Services**

## I. OVERVIEW

This policy applies to all SUNY Downstate Medical Center (SUNY DMC) and it's affiliate employees, contractors, and other authorized 3rd party entities who use the SUNY DMC computer network.

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal business operations in addition to the possibility of placing patient care at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Given the large number of computer workstations and servers that comprise the SUNY Downstate network, it is necessary to leverage a comprehensive patch management solution that can effectively distribute security patches automatically when they are made available. The patch management solution has the ability to evaluate individual computer workstations and servers for vulnerabilities. Patches may then be automatically installed and, when necessary, the affected machine rebooted. The patch management solution further facilitates regulatory compliance with HIPAA and NY State law by providing extensive audit capabilities that record all remediation transactions.

Effective security is a team effort involving the participation and support of every SUNY DMC employee and affiliate who is a user of the SUNY DMC computer network. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly as is required by law.

## II. PURPOSE

The purpose of this policy is to outline the requirement that all network computers have a centrally administered ID and password that is accessible to Downstate IS department. This policy also outlines the conditions under which this ID will be used.

## III. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at SUNY DMC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SUNY DMC.

## IV. POLICY

### Central Password and Patch Policy

- **a.** While SUNY DMC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of SUNY DMC. Due to the need to protect SUNY DMC's network, the management cannot guarantee the confidentiality of information stored on any network device belonging to SUNY DMC.
- **b.** All computers must have the latest Service Packs and Security Patches installed.
- **c.** All computers must have an ID designated by the IS department joined to the Local Administrator Group or equivalent of the computer that facilitates appropriate patch management.
- **d.** All users must agree to have their computers scanned for software versions, have the appropriate version downloaded, and if the situation requires, have the computer rebooted by patch management software.
- **e.** SUNY DMC recommends that any information stored on individual workstations that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see SUNY DMC Information Sensitivity Policy. For guidelines on encrypting e-mail and documents, refer to the SUNY DMC Awareness Initiative.
- **f.** For security and network maintenance purposes, authorized individuals within SUNY DMC may monitor equipment, systems and network traffic at any time, per the SUNY DMC audit policy.
- **g.** SUNY DMC reserves the right to audit networks and systems to ensure compliance with this policy.

## V. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## VI. DEFINITIONS

## VII. REVISION HISTOIRY

## VIII. REASONS FOR CURRENT REVISIONS

- o Changes in regulatory or statutory have laws or standards
- o System failures/changes
- o Institutional/operational changes

## IX. ATTACHMENTS:

## X. REFERENCES:

JCAHO Standards

| Date Reviewed | Revision Required (Circle One) | | Responsible Staff Name and Title |
|---|---|---|---|
| | Yes | No | |
| | Yes | No | |
| | Yes | No | |
| | Yes | No | |