



## **ASU Patch Management Standard**

Version 0.1  
November 2008

## Table of Contents

1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL .....	3
2 DOCUMENT REVISION .....	3
3 DEFINITION OF TERMS .....	4
4 STANDARD.....	4
5 ENFORCEMENT.....	4

## 1 Document Classification: University Confidential

Physical and Administrative Controls	Reproduction	Distribution	Destruction/Disposal
Each employee is responsible for controlling usage and access on a need-to-know basis. This policy also applies to contractors.	Limited copies may be made only to employees or contractors who have signed a non-disclosure agreement.	Internal: Use University envelope whenever possible. External: Use sealed envelope.	Use document destruction bins. Shred or erase magnetically recorded documents if unable to recycle.

## 2 Document Revision

Date	Revision	Revised By	Basis for Revision & Description

### Document Change/Correction Request

Your feedback is valuable. Anyone who uses this document is invited to use this form to submit requests for changes or corrections to this document. Please complete all of the sections and mail to:

#### Document Identification

Document title  
Date of Document  
Master File Location

#### Requester Identification

Name	
Department	
Phone Number	( ) -
Email Address	

#### Request

The following Change is requested:

Please describe the change and reason(s) why the change is requested.

Correction:

Section \_\_\_\_, page \_\_\_\_ contains the following erroneous information:

This information should be changed to:

Attach additional sheets if necessary to fully describe the change or correction.

### 3 Definition of Terms

An **Operating System (OS)** is the set of programs used to provide the basic functions of a computer.

A **device** is defined as any object used to store, process, and/or transfer data.

A **networked device** is defined as any device that is either permanently or periodically attached to the Indiana University network.

**Remediated** is defined as the application of all patches required by the vendor.

**Mitigated** is defined as the steps taken to protect a device from a particular vulnerability, i.e. the device has been removed or otherwise isolated from the network, the NIC card has been removed, or an approved deviation from the required patch process has been approved by the Information Security Officer (ISO) and is on file.

### 4 STANDARD

All networked devices belonging to ASU entities and/or managed by the University Technology Office (UTO), practice plans, or other affiliated and partner organizations will be patched with vendor provided operating system security patches.

These patches will be applied as soon as possible following appropriate testing of the security patches by the ASU entities and/or managed by UTO, practice plans, or other affiliated and partner organizations.

New devices must be patched to the current patch level as defined by the operating system vendor *prior* to the device being connected to the production network.

Current patch status for all ASU entities and/or managed by UTO, practice plans, or other affiliated and partner organizations must be communicated to the Information Security Officer or designee. Devices that cannot be patched will report the exact mitigation effort to the Information Security Officer or designee.

### 5 ENFORCEMENT

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