Villanova University **No. 7310 Rev.: Approved**
Information Technology Policy and Procedures **Date: January 27, 2016**

Subject: Patch Management Policy

Table of Contents

1. Purpose

Villanova University is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactively managing vulnerabilities will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred.

The purpose of this policy is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform the University community about the change in end point computing.

2. Policy Statement

2.1 Enterprise Servers

All servers under UNIT control will be maintained with the latest security patches to their operating systems and key applications.

Each business unit is responsible for devices and systems under their control. Business unit directors must ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list or by direct notification from the vendor. When a patch is announced, an authorized system administrator must enter a change ticket according to the change management policy. When the ticket is entered, a criticality rating of either high or normal must be assigned. Criticality ratings are usually supplied by vendors, but in the case that no criticality is supplied, the system administrator must assign a rating based on his/her experience. All high/critical patches must be applied as soon as practically possible, but not longer than thirty (30) calendar days after public release for any critical production server. All patches that are medium/high severity or for non-critical systems must be rolled out within ninety (90) calendar days. Any low priority patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.

In the case where patches cannot follow the aforementioned schedule, a document must be produced explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at that time. Any patches which are to be deferred longer than the scheduled timeframe must be approved by the Chief Information Security Officer (CISO) or his/her assignee. All deferred patches must be reviewed at least quarterly.

All patches for vendor maintained systems/applications that are labeled as high/critical and apply to security must also be patched within 90 days of the approved release from the vendor. Any functional but non-critical patches may be installed on a case-by-case basis. UNIT is responsible for maintaining knowledge of these patches and ensuring that vendors comply with our internal policy.

Business unit directors are responsible for performing a vulnerability scan on their systems after each patch window to show that the patches were installed correctly. Clean vulnerability scan reports should be submitted to the CISO quarterly for review.

2.2 Endpoints

All University-owned Windows based endpoints are to have critical operating system and key application patches installed within 30 days of release from the vendor.

3. Scope

This policy applies to all Enterprise Servers which are owned by the University. It also applies to University-issued Windows endpoints bound to Active Directory (VUAD).

4. Procedures

4.1 Scheduling and Deployment

Software vendors release security patches on a regular schedule. Applicable patches will be tested and validated by UNIT prior to deployment to campus. Once validated, UNIT will schedule and deploy validated patches to end points on a monthly basis. Communication to campus regarding deployed security patches will be done through Campus Currents.

4.2 Installation and Validation

A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. UNIT understands the impact an ill-timed reboot can have on user productivity. In order to provide the University community with as much flexibility as possible, security updates will be deployed using an “optional-mandatory” method.

The optional-mandatory method will allow users to install scheduled update at their convenience before a deadline occurs. Users will be provided **five (5) business days** to select the installation time of their choosing for deployed patches. After the deadline passes, updates will automatically install and may enforce reboots of the computer as the updates require. It is strongly recommended that users install the updates as soon as possible to ensure that end points are protected and rebooting does not disrupt work. When updates are available, a notification will appear in the system tray. The message will continue to appear daily until the updates are installed and will appear more frequently as the deadline approaches.

4.3 Out of Band Updates

On occasion a software vendor will release a highly critical security patch outside of their normal release cycle. The usual reason for the release of an out-of-band patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out of band patch, UNIT will expedite the validation process. Once validated, users will have one **(1) business day** to install and reboot their machine to apply the patch. After the deadline passes, updates will automatically install and may enforce reboots of your computer as the updates require. UNIT will communicate to the campus via Campus Currents in the event of an out of band update deployment.

4.4 Mandatory Reboot Exemption

There is the possibility of academic or administrative processes being negatively impacted even with a five-day window for users to apply patches. Users who could be impacted in this scenario may contact the University Helpdesk and request to be temporarily exempted from the mandatory reboot process. The endpoints being exempted will still have patches deployed regularly, but it will be the responsibility of the end user to reboot the machine to apply those security patches. Each request will be reviewed on a case by case basis and will have a limited duration for exemption.

5. Definitions

University-owned devices are defined as any device which was purchased by the University and is currently being managed by University IT (UNIT). These devices include but are not limited to, any laptop or workstation which was deployed to faculty or staff by UNIT. This excludes any personal (BYOD) device which may be connected to the University computer network.

6. Approval and Revisions

Version 1.0 approved February 10, 2016 by VP&CIO Stephen Fugale and the University Council on Information Technology (UCIT).