New Jersey Institute of Technology

Information Services & Technology Division

Patch Management Standard

Table of Contents

1.0 Standard Statement

New Jersey Institute of Technology (NJIT) Information Services & Technology (IST) division is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised device threatens the integrity of the network and all computers connected to it.

NJIT IST is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. The IST division attempts to provide appropriate protection against cybersecurity threats, such as viruses, malware, ransomware, phishing, and compromised credentials which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this standard will limit the exposure and effect of common cybersecurity threats to the systems within this scope.

To combat this threat IST has implemented a patch and vulnerability management process. This process includes continuous vulnerability scanning and assessment performed by automated tools and members of IST. 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.

This document describes NJIT's requirements for maintaining reliable and secure IT Services, this includes but is not limited to operating systems,applications, firmware, and security patches on all University owned and managed endpoint devices, servers and network devices. The goal is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates.

2.0 Scope

This Standard applies to workstations, servers and any network devices owned, used, managed by NJIT and any vendors, contractors, partners doing business with the university. This includes all systems and applications used by both on premise and in the cloud services that contain data owned or managed by NJIT regardless of location. The scope also include but is not limited to, any laptop or workstation which was deployed to faculty or staff by IST. This excludes any personal (BYOD) devices which may be connected to the University computer network. BYOD devices will follow the guidelines laid out in the acceptable and responsible use policy (ARUP). BYOD devices are expected to follow best practices for software updates. NJIT IST reserves the right to block devices from the network that may cause harm to NJIT information assets and resources.

3.0 Security Ratings

NJIT Risk	Description	CVSS V3 Score Range*	Definition	Security Impact
Critical	This rating is given to flaws that could be easily exploited by an attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that dictate immediate remediation.	9.0 - 10.0	Exploitation is straightforward and usually results in system level compromise. It is advised to form a plan of action and patch immediately	Loss of CIA (Confidentiality, Integrity, and Availability) is likely to have the highest severity of adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
High	Flaws that can compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.	7.0 - 8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.	Loss of CIA (Confidentiality, Integrity, and Availability) is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Moderate	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the	4.0 - 6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and	Loss of CIA (Confidentiality, Integrity, and Availability) is likely to have a serious adverse effect on the organization or individuals

	types of vulnerabilities that could have had a Critical or High but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.		patch after high-priority issues have been resolved.	associated with the organization (e.g., employees, customers).
Low	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.	0.1 - 3.9	Vulnerabilities are not exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.	Loss of CIA (Confidentiality, Integrity, and Availability) is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
*CVSS V3 - The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease and impact of an exploit. Scores range from 0 to 10, with 10 being the most severe. (en.wikipedia.org)				

4.0 Standard

4.1 Servers

All servers containing NJIT information resources will be maintained with the latest security patches to their operating systems and applications. Servers must comply with the minimum security standards that have been approved by IST. These minimum security standards define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the University asset and the data that resides on the system. Before a system is put into production system owners are responsible for performing a vulnerability scan on their systems to ensure they meet security and patch level requirements.

Each department is responsible for devices and systems under their control. Directors must ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list, by direct notification from the vendor, by the result of a vulnerability scan, scheduled patch scan, or other notification.

- *Recognizing the fact that critical category patches are often released quickly and shortcut quality controls, IST must validate impact before applying these patches. Patching for critical vulnerabilities is often a very dynamic situation with vendors recalling and re-releasing patches multiple times.*
- *For all Critical and High severity ratings, remediation countdown timers begin from the date of public release of patch or mitigation. Moderate to Low level severity ratings remediation countdown timers begin from the date of last scheduled vulnerability or patch scan.*

Severity Rating	Time to Remediate
Critical	As soon as possible(normally within 24 hours), no longer than 5 calendar days after public release.
High	As soon as possible, no longer than 30 calendar days after public release
Moderate	No longer than 60 days
Low	No longer than 90 days

All patches should be tested on development and/ or test systems before being rolled out to production, where possible, or if approved by the Chief Information Officer (CIO) or his/her designee.

In the case where patches cannot follow the aforementioned schedule, a document must be produced explaining why the patch must be deferred. Any patches which are to be deferred longer than the scheduled time frame must be approved by the CIO or his/her assignee. All deferred patches must be reviewed by the CyberSecurity Working Group (CWG).

4.2 Endpoints

All University-owned based endpoints are to have critical operating system and key application patches installed within 30 days of release from the vendor. Desktops and laptops must have automatic updates enabled for operating system patches. This should be the default configuration for all workstations. Any exception to the Standard must be documented and forwarded to CWG for review and approved by the CIO or his/her assignee.

4.3 Network Infrastructure and other network attached devices

All network infrastructure and network attached devices will be maintained with the vendor recommended code updates to their systems and key applications (if applicable). Updates will be applied when a vulnerability has been disclosed and is made available from the manufacturer. Other security mitigations will be enabled if an update can not be completed in a timely fashion because of potential network downtime.

4.4 Critical business systems and enterprise applications

All critical business systems and enterprise applications (i.e. Ellucian Banner, Canvas, etc.) will be maintained with vendor recommended code updates to their systems and key applications including both on premise and in the cloud services that contain data owned or managed by NJIT. Updates will be applied when a vulnerability has been disclosed and an update released from the vendor. Other security controls and remediations will be implemented if an update or a patch can not be completed in a timely manner to mitigate the risk. Any exception must be documented and forwarded to CWG for review and approved by the CIO or his/her assignee.

5.0 Procedures

5.1 Scheduling and Deployment

Applicable patches will be tested and validated by IST prior to deployment to campus. Once validated, IST will schedule and deploy validated patches to systems following patch cycle and scheduled maintenance window. If a service or application is to become unavailable for a significant amount of time appropriate approvals will be requested from campus partners, and a communication to the campus regarding the outage will be done following NJIT guidelines.

5.2 Installation and Validation

Software vendors release security patches on a regular schedule. A system reboot is required to successfully install many security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. IST 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 for **windows based endpoints** (desktops, laptops) will be deployed using an “optional-mandatory” method.

The optional-mandatory method will allow users to install scheduled updates at their convenience before a deadline occurs. Users will be provided **ten (10) 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 endpoints 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

5.3 Critical Updates

On occasion a software vendor will release a highly critical security patch. IST will expedite the validation process. Critical patch that needs emergency request for change and should be applied as soon as possible. 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. IST will communicate to the campus in the event of an out of band emergency update deployment to the systems that would force a reboot.

5.4 Scheduled Maintenance Windows

A maintenance window is a regularly scheduled timeframe during which planned outages and changes to production may occur except during the time of change restrictions, i.e. academic schedules and administrative events, etc. The purpose of defining recurring maintenance windows is to set the expectation by providing stakeholders with predictable periods of disruption to the offered services. A maintenance window is reserved for a pre-approved outage time which the impacted campus partner(s) will be notified prior to the schedule. It does not mean that all the impacted systems or services will always be down during this time. It will be used when needed, along with appropriate approval and campus communication.

All planned outages are prioritized over the service impact level defined as Critical, High, Moderate, and Low. Any IST Service disruption will follow the process accordingly except emergency situations and unplanned downtime. The following are the scheduled maintenance windows defined to manage patches throughout the patch cycles for IST systems and services:

Cadence	**Duration**	**Day/Time**	**Impact**
Production			
Daily	1 hour	Daily - 5am-6am	Low - None (minutes)
Weekly	4 hours	Saturday 11pm - Sunday 3am	Moderate (1-4 hours)

Monthly	8 hours	Last Saturday of the month 11pm - Sunday 7am	High (up to 8 hours)
Non-Production (User Facing)			
Daily	2 hours	Daily - 7pm-9pm	Low
Monthly	8 hours	2nd Tuesday of Every month, 9am-5pm	Moderate