Northwestern
INFORMATION TECHNOLOGY

Approving University Official(s): Vice President for Information Technology/Chief Information Officer
Responsible Office: Information Security
Effective date: September 1, 2022

Patch Management Standard

1. Summary

The Patch Management Standard (hereafter referred to as the "Patch Standard") outlines the necessary actions each person or organization who is responsible for the protection of University IT assets and data is required to perform in order to protect the integrity of the systems and data for which Northwestern is responsible.

This **Patch Standard** is intended to prevent the loss or compromise of Institutional Data, meet regulatory and contractual requirements, meet minimal data protection hygiene standards, as well as ensure that devices on the Northwestern University network are not used to attack other systems, both at Northwestern and on the Internet.

2. Authority

The authority for implementation and enforcement of this Standard is based on the Information Security Policy, effective January 1, 2022.

3. Purpose Statement

All devices connected to a Northwestern University network (physical wired connection or wireless) (hereafter "University Network") or used for University Business, including personal devices, must apply security patches on a schedule appropriate to the level of risk that they mitigate.

4. Scope and Audience

The systems scope of this Patch Standard applies to all information and communication technology (ICT) that connect to a University Network. The audience of this Patch Standard include all employees, faculty, staff, students, affiliates, suppliers, and anyone else accessing a University Network.

This Patch Standard also applies to cloud-hosted applications under the control of Northwestern or applications with a direct connection to a University Network (e.g. site-to-site VPN, network tunnel, or

Direct Data Center cross-connect). Vendors who have completed a Northwestern Service Provider Security Assessment (NU SPSA) are evaluated on their patching procedures, and the responses inform the risk assessment process.

5. Control Requirements

The specific control requirements, controls, and capabilities that must be implemented are dependent upon the risk posed, the data processed, and the University's contractual and regulatory compliance obligations.

For ICT devices connected to Guest Wireless Network (SSID Guest-Northwestern)

Although Northwestern recommends that all devices have appropriate security patches in place for software and operating systems, at this time there are no requirements that Guest connections and devices must have appropriate security patches implemented.

For all ICT devices connected to a University Network, or used for University Business, except for Guest Wireless:

1. All devices connected to a University Network (including personal devices) or used to conduct University Business must only run supported software and operating systems for which security patches are made available in a timely fashion.
2. Software or operating systems that are deemed "end of life" by a vendor, manufacturer, or developer, without the option for extended support are not permitted on a University Network without an exception approved by the Information Security Office (ISO).
3. All devices connected to a University Network will adhere to the following Patching Schedule, which is based on the National Vulnerability Database (NVD) ratings and the Common Vulnerability Scoring System (CVSS):

Severity Rating	CVSS Base Score	Plan of Action Created Within	Patches Applied Within
Critical	9.5-10.0	48 hours	5 days
High	7.0-9.4	3 days	10 days
Medium	4.0-6.9	15 days	30 days
Low	0.0-3.9	30 days	90 days

4. Plans of Action (POA) must be created within the timeframe listed above from *when the vulnerability is published and scored by the NVD*. POAs need not be detailed in all cases, however, for complex applications or architecture timelines, milestones, and interim mitigations will be required.
5. Patches must be applied within the timeframe listed above *from when the vulnerability is published and scored by the NVD.* In instances where patches for a given vulnerability are not available in the timeframe provided, official mitigations or workarounds provided by the vendor/manufacturer must be applied in the same timeframe. When a patch is made available, it must also be applied within the timeframe listed above based on its date of release.
6. If a vulnerability is identified and an official CVSS score from the NVD is not available, the Information Security Office (ISO) will perform a risk analysis of the vulnerability based on the *exploitability, scope, and impact* of the vulnerability to Northwestern specifically. If the results of

the analysis indicate the equivalent of **High or Critical** severity rating, the ISO will communicate the requirement to for the university community to remediate the vulnerability in the timeframes listed above. The timeframe for when Plans of Action or applying patches is required will be measured from the time in which the ISO communicates the requirement to the university community.

7. Exceptions to this schedule can be requested if there are mitigating controls that are in place to reduce risk, such as devices not having access to the public Internet or the entire University Network. Requests for exceptions can be submitted to the Information Security Office and must include specific lists of devices as well as the mitigating controls in place. This may be required for certain research labs and other devices that cannot upgrade their software or operating systems.
8. Patch management processes must be in place to:
    8.1. Identify all ICT devices and their current and available security patches,
    8.2. Evaluate and test available security patches,
    8.3. Install security patches and confirm the success of the installation.
    8.4. Remove previous versions of software and firmware components after updated versions have been installed.
9. Patching should only be performed by organizational personnel with authorization for appropriate privileged access to ICT.
10. University-owned devices should, whenever possible, leverage endpoint management and automation provided by Northwestern Information Technology or Schools/Business Units, as patching is an ongoing, recurring activity.

6. Standard Implementation

The following are recommended practices for ensuring compliance with the requirements outlined in this Patch Standard.

Northwestern Information Technology, as well as multiple distributed Schools and Business Units, offer patch management services for endpoints that are automated. These services are available for all Northwestern-owned devices and include the following software:

- **JAMF Pro:** Provides operating system updates and patch management for macOS, iOS, and iPadOS devices. This includes the operating system as well as installation and management of third-party software.
- **KACE:** Provides third-party software installation and patching for popular business and productivity software on Windows devices such as Adobe products, Firefox, Chrome, Zoom, and others.
- **WSUS:** Provides patching and updates for Microsoft products (primarily Windows and Office).
- **Ansible:** Provides patching and updates for Enterprise, hosted and managed Linux servers at the University Data Center.

For personal devices, the following settings can be enabled to ensure patches are installed in a timely manner:

- Microsoft Automatic Updates
- Apple Automatic Updates
- Automatic updates for common productivity software such as Adobe Acrobat, Zoom, Chrome, and Firefox.

Monitoring of alert feeds for patching is also important – the following are good resources for how to maintain awareness of critical patches:

- Northwestern IT SEC-UNITS Mailing List
- Apple Security Updates: https://support.apple.com/en-us/HT201222
- Microsoft Security Updates: https://docs.microsoft.com/en-us/security-updates/
- CISA (Cybersecurity and Infrastructure Security Agency) Alert Feeds: https://www.cisa.gov/uscert/mailing-lists-and-feeds
- Red Hat Customer Portal: https://access.redhat.com/security/security-updates/#/security-advisories
- Ubuntu Security Notices: https://ubuntu.com/security/notices

Please contact Northwestern IT – Endpoint Device Management to learn more or enroll in these services. If you're unsure if your Northwestern-owned endpoint devices are managed, you can contact your local IT support or Northwestern IT for more information.

7. Remedies and Compliance

In order to demonstrate Northwestern's security posture and patching status, the Information Security Office is authorized to require verification of compliance for any ICT device connected to a University Network. Such verification may be in the form of a system report, an authenticated vulnerability scan, a penetration test, or an approved Exception Request.

In the event of non-compliance with this Patch Standard, the Information Security Office may escalate the issue to School/Unit Senior Leadership.

In the event of continued or persistence non-compliance with this Patch Standard, the Information Security Office, in consultation with the Information Security Advisory Committee, may disconnect systems from the University Network until the system can be patched or adequate remedies put in place.

8. Definitions

Information and Communication Technologies (ICT): An umbrella term used to describe all information and communication technologies, that includes, but is not limited to, the Internet, wireless technologies, software, systems, applications, public/private/hybrid cloud, computers, social network, as well as other media applications and services. See https://csrc.nist.gov/glossary/term/information_and_communication_technology.

Information Security Advisory Committee (ISAC): A University-wide technology governance group that is responsible for monitoring the security maturity and controls of the University, and providing approval for all security vulnerability exceptions that pose a significant or high risk to the University.

Institutional Data: All data that the University is responsible and accountable for protecting. This data includes, but is not limited to, data the University owns collects or licenses, intellectual property owned by faculty or others, staff data, student data, faculty data, research data, personal information, alumni data,

vendor and contractor data, and data that the university shares or provides to third-parties for storage, processing, and analysis.

Internet of Things (IoT): A device (or group of devices) that contain the hardware, software, firmware, sensors, or other actuators which allow the devices to connect and exchange data with each other or the Internet. See https://csrc.nist.gov/glossary/term/internet_of_things_IoT.

Northwestern- or University-owned Devices: ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are the responsibility of the University to account for and provide appropriate safeguards. This includes ICT purchased (either directly or by reimbursement) from a University chart of accounts, or devices with documented ownership or responsibility transferred to the University from another institution or organization (such as ICT loaned to a laboratory or department).

Personal or Personally-owned Devices: ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are wholly owned by an employee, student, or affiliate of the University. This includes devices for which a user receives a stipend or subsidy, such as a mobile communication allowance.

For purposes of this Patch Standard, ICT both not owned by Northwestern and not wholly owned by an employee, student, or affiliate (such as ICT that belongs to another company or institution) are considered Personally-owned Devices.

University Network: The University Network is the infrastructure and equipment that connects information and communication technology (ICT) to enable the exchange of data and information at Northwestern. This includes connections that are limited to within the university as well as the broader Internet. The University Network includes both physical wired (wall jacks, wiring, routers, switches, etc.) and wireless network components, including ad-hoc wireless networks. The University Network also includes connections provided by a third-party telecommunications provider but managed by Northwestern IT, or network paths over hardware or software (such as VPN, site-to-site tunnel, etc.) by which a user or ICT device receives a Northwestern-managed IP address, telephone number, or other Northwestern-owned network descriptor.

For purposes of this Patch Standard, the Guest Network (SSID: Guest-Northwestern) is not considered a University Network.

University Business Any activity carried out under the auspices of Northwestern University and in furtherance of the University's mission.

9. Related Policies, Standards, Guidelines or Procedures

Information Security Policy
Appropriate Use of Electronic Resources

10. Contact Information

The following office can address questions regarding this Standard:

Northwestern Information Technology, Information Security Office
email: security@northwestern.edu

11. Revision History

Date	Version	Modified by	Comments
July, 2022	1.0	Northwestern IT/ISO	New

12.Standard URL:

https://www.it.northwestern.edu/policies/patchmanagement.html

13. Support Services – Patch Management and Mitigation Strategies

Northwestern IT is committed to providing services and resources that will enable our community to protect the integrity of its systems and data. Therefore, the following resources are available to enable patch management of Northwestern-owned computer equipment:

1. **School/Unit Automated Patch Management or Firewall Services**
   Several schools and units across Northwestern offer patch management or network security solutions that are tailored specifically to the unique needs of their faculty and staff. Please contact your local IT support to find out what services may be available in your school or unit.
2. **NUIT Endpoint Management – Full Automation**
   The Endpoint Management (EDM) team can automate patching on University-owned Mac or Windows devices on a regular basis. The general schedule for patching is once every 30 days, with a frequency that will be communicated in advance. In the event of zero-day or critical security patch requirements, additional communication will be provided to the community. This service is available to groups that manage multiple university-owned endpoint devices at no incremental cost to the group or department. For more information on this service, please email consultant@northwestern.edu.
3. **NUIT Endpoint Management – Notification Only**
   For sensitive laboratory equipment or other devices that will not support automatic patching, the EDM team can provide reporting on Mac and Windows devices that fall out of compliance. Installation of patches will remain the responsibility of the end user or department, however, such notifications will help units prioritize remediation of systems. This service is available to groups that manage multiple university-owned endpoint devices at no incremental cost. For more information on this service, please email consultant@northwestern.edu.
4. **NUIT Endpoint Management – Custom Solutions**
   NUIT Technology Support Services can work with individual, units, or groups to develop a customized patch management program. This service operates on a cost recovery model, depending on the level of customization that is required. For more information about this service, please email consultant@northwestern.edu.
5. **Network Firewall Services – Default Deny**
   Northwestern IT provides border-level firewall services that deny unsolicited inbound traffic from the Internet. This service is provided to the community at no incremental cost. More information about this service is available here: https://www.it.northwestern.edu/network/duit/index.html.
6. **Network Firewall Services – Managed Solutions**
   Northwestern IT provides managed firewall services with custom rulesets that can mitigate vulnerabilities or isolate hosts that are unable to be secured, patched, or run a current operating system. Charges for this service varies based on the complexity of the organization and bandwidth requirements. More information about managed firewall solutions is available at https://www.it.northwestern.edu/service-catalog/security/secure-computing/firewall.html.