Patch Management Policy for Chicago State University Systems

Policy Statement

Regular application of vendor-issued security updates and patches are necessary to protect CSU data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices routinely require patching for functional and secure operations.

Purpose

The purpose of this policy is to ensure CSU reduces risks resulting from exploitation of published technical vulnerabilities. Software is critical to the delivery of services to CSU customers and CSU users. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

Scope

The CSU Patch Management Policy applies to any all wholly owned ITD resources in the CSU environment.

Definitions

- **University-Related Persons / Employee / Staff** are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University.
- **Associate / "Extra Help", Third-party or 3rd party** is someone officially attached or connected to the College who is not a student or employee (e.g., Extra Help, vendors, interns, temporary staffing, volunteers.)
- **ITD Resources / Information Resources** - include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, security, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
- **Information System** is a major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

- **Information Technology Department** is the individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.
- **Unit** is a college, department, school, program, research center, business service center, or other operating component of the University.
- **A patch** is a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:
    - Updating software
    - Fixing a software bug
    - Installing new drivers
    - Addressing new security vulnerabilities
    - Addressing software stability issues
- **Patch management cycle** is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Patch management occurs regularly as per the Patch Management Procedure.
- Information Technology Department to stay in line with our internal naming convention. **ITD** Technology Department **University Information** is any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.
- **Security Awareness Training** - The formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about institutional policies and procedures for working with information technology (IT).
- **Personally Identifiable Information (PII)** - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
- **Education records under FERPA**, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the College.
- **Health Insurance Portability and Accountability Act (HIPAA)** - Demands that all HIPAA covered businesses prevent unauthorized access to “Protected Health Information” or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.
- **Gramm-Leach-Bliley ACT (GLBA)** - Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data.

- **Functional Lead** - Technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to ITD.
- **The Family Educational Rights and Privacy Act (FERPA)** - a federal law that protects the privacy of student education records.
- **Information Owner** - is a person responsible for the management and fitness of information elements (also known as critical data elements) - both the content and metadata.
- **Backup** is saving or copying information onto digital storage media.
- **Restore** is performed to return data that has been lost, stolen, or damaged to its original condition or to move data to a new location.
- **Recovery Point Objective** (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.
- **Recovery Time Objective** (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.
- **Electronically stored information (ESI)** is the general term for any electronic information stored on any medium (i.e., hard drive, back-up tapes, CDs, DVDs, flash drives, external drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
- **Archive** is defined as the saving of old or unused files on off-line mass storage media for the purpose of releasing on-line storage space.
- **Disaster Recovery** is a combination of the policies, process and procedures related to preparing for recovery of technology infrastructure critical to CSU operations after a natural or human induced event. Disaster recovery focuses on the restoring technology systems that support business functions that fail in the event of a disaster.

Responsibility

University-Related Persons / Employee / Staff, Associate / "Extra Help", Third-party or 3rd party

Are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

Information Technology/Technology Department

Are responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by ISO, and for enabling and participating in validation efforts, as appropriate.

Information Technology Department Leader

ITDTD must, at the direction of the Information Security Program Leader:

- identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics;

- develop, establish, maintain, and enforce information security policy and relevant standards and processes;
- provide oversight of information security governance processes;
- educate the University community about individual and organizational information security responsibilities;
- measure and report on the effectiveness of University information security efforts; and
- delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

Policy

1) General

CSU shall:

a. Ensure all non-legacy applications are fully supported by the manufacturer.
b. To the greatest extent possible, maintain all support and maintenance agreements for the lifetime of the application.
c. Obtain timely information about technical vulnerabilities of information systems and applications being used.
d. Take appropriate, timely measures to address the associated risk, including patching vulnerabilities.

As set forth below, CSU management of technical vulnerabilities is supported through the use of the controls set forth in:

a. Vulnerability risk assessment (see Section 2.0 below).
b. Vulnerability scanning (see Section 3.0 below).
c. Patch management (see Section 4.0 below); and
d. Security alerts, advisories, and directives (see Section 5.0 below).

2) Vulnerability Risk Assessment

CSU shall:

- Update the risk assessment on a defined schedule or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system; and
- Establish expected patching timelines based on the risk assessment.
    - Patching of security vulnerabilities must be completed as soon as adequate testing has been done to ensure risk of adverse impact due to patch deployment is less than risk of impact from vulnerability exploit.
    - Patching of security vulnerabilities must occur within two weeks of patch release unless some justifiable reason for not doing so exists.
    - Patching addressing vulnerabilities that are being actively exploited must be tested and deployed within forty eight hours.

- Non security related patches, such as ones that provide additional functionality or address performance issues, should be completed as soon as adequate testing has been completed if the issue the patch addresses is being experienced and/or if the additional functionality is desired.

3) Vulnerability Scanning

CSU shall:

- Scan for vulnerabilities in its information system and hosted applications in accordance with a defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws and improper configurations;
  - Measuring vulnerability impact using a defined method;
  - Reporting and providing clearly documented and defined results;
  - Identifying code-based vulnerabilities; and
  - Identifying configuration-based vulnerabilities.
- Analyze vulnerability scan reports and results from security control assessments;
- Remediate legitimate vulnerabilities in accordance with its assessment of risk; e. share information, when appropriate, obtained from the vulnerability scanning process and security control assessments with designated personnel throughout CSU to help eliminate similar vulnerabilities in other information systems;
- Employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned;
- Update the list of information system vulnerabilities scanned or when new vulnerabilities are identified and reported;
- Attempt to discern what information about the information system is discoverable by adversaries;
- Include privileged access authorization for selected vulnerability scanning activities to facilitate more scanning;

Was this in the finding?

Due to the interdependency of the CSU network and resources, any vulnerability assessment scan shall be performed in cooperation with the CSU ITD and shall follow defined and approved procedures for running such scans.

3.0 Patch Management and Flaw Remediation

CSU shall:

- Identify, report and correct information system flaws;
- Test software updates and patches related to flaw remediation for effectiveness and potential side effects on the CSU information systems before installation;

- Incorporate flaw remediation and patch management into its configuration and change management process;
- Develop processes for assessing the success and extent of patch management efforts;
- Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe;
- And if automated tools cannot be used, develop process for provisioning updates and ensuring updates are deployed.

4.0 Security Alerts, Advisories and Directives

CSU shall:

- Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
- Generate internal security alerts, advisories and directives as deemed necessary;
- Disseminate security alerts, advisories, and directives to appropriate personnel; and
- Implement security directives in accordance with established time frames.

Miscellaneous

This policy shall supersede all previous CSU technical patch or vulnerability management policies. This policy may be amended or revised at any time. Users are responsible for periodically reviewing this policy for any revisions and for adhering to those revisions. This information is set forth in the CSU Scope, Background and Governance Statement for Information Security Policies. DEFINITIONS Terms used in this policy are defined in the CSU Information Security Glossary.

Policy Exceptions and Maintenance

Waivers from certain and specific policy provisions may be sought following the CSU ITD approval Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted by the ITD.

Enforcement

This Patch Management Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between CSU policies, they must be brought to the attention of CSU for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.

References

- NIST CSF: ID.RA-1, PR.IP-12, DE.CE-8

Version History

Version	Modified Date	Next Review	Approved Date	Approved By	Comments
1.0	11/3/2022	11/1/2023	11/6/2022	Donna Hart	