



## Patch Management Policy for Chicago State University Systems

Policy Statement secure operations.

### Purpose

The primary purpose of this policy is to ensure CSU's critical information systems, software, and hardware are protected from security vulnerabilities. Regular updates are critical to maintaining system security.

### Scope

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



- x 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.
- x Unit is a college, department, school, program, research center, business service center, or other operating component of the University.
- x 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.



- x Functional Lead Technical lead point person for department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to IT
- x The Family Educational Rights and Privacy Act (FERPA) Federal law that protects the



- x develop, establish, maintain, and enforce information security policy relevant standards and processes;
- x provide oversight of information security governance processes;
- x educate the University community about individual and organizational information security responsibilities;
- x measure and report on the effectiveness of University information security efforts; and
- x





- x Incorporate flaw remediation and patch management into its configuration and change management process;
- x Develop processes for assessing the success and extent of patch management efforts;
- x 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;
- x 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:

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

## Miscellaneous

This policy shall supersede all previous CSU technical or vulnerability management policies. This policy may be amended or revised at any time. Users are responsible for periodically

## Policy Exemption and Maintenance

Waivers from certain exceptions...

## Enforcement

This policy supplements and complements other related information security policies, it does not supersede any such policy or vice versa. Where there are any

