

## Patch Managemer Policy for Chicago State University Systems

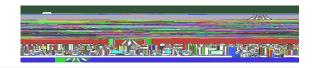
Policy Statemestecure operations.

#### Purpose

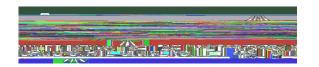
The properties and the strict of the properties of the properties

#### Scope

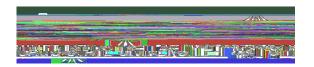
The CSU Patch Management Policy applies to any all wholly owned ITD resignatings SSU environment.



- x Information Technology Departments 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 acollege, department, school, program, research center, business service center, or other operating component the University.
- x A patchis a software update comprised code inserted (i.e., patched) into the code of an executable program. Typicallypatch is installed into an existing software program. Patches are often temporary fixes between full releases onfsees ao2fmbl( re)9 ()10 (tn)-7 (nfe

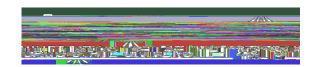


- x Functional Lead Technical lead point person fordepartment. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to IT
- x The Family Educational Rights and Privacy Act (FERPRe)derallaw that protects the



- x develop, establish, maintain, and enforce information security policyraled ant 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 Unisity information security efforts; and

Х



- x Incorporate flaw remediation and patch management into its configuration and change management pocess;
- 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

#### CSUshall:

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

#### Miscellaneous

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

#### Policy Exeption and aintenance

Waivers from certain anspe.1 (i)4 (f(;)-1.1 ()10.1 (()2 (y)4.1 (;)-1.1 ()])4 (allisr 4 (o)2 (2 (e)-8>Tj7513

### En688.7 (o)1.5 (r)-7.9 (c)-1.9 (e)-(e)ment

This Pat.1 (h Miw)2 9i Wehroet supplements and compliments ather related info.1 mation security policies, it do.1es not supersede any such policy o.1 vice versa. Where there are any