Policy Name	Patch Management Policy
Policy Number	50000.019
Effective Date	January 25, 2019
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	March 11, 2022

1. Policy Statement

   The purpose of this policy is to provide the processes and guidelines necessary to maintain the integrity of critical systems and end user systems campus-wide and Jackson State University's data by applying the latest operating system and application security updates/patches in a timely manner.

2. Definitions

   2.1. Patches- Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product.

3. Scope

   This policy and its processes refers to all JSU owned desktops, laptops, servers, applications, mobile and network devices and any other additional items that represent access points to sensitive and confidential University data as well as to technology resources and services.

4. Employee Adherence

   This policy applies to all JSU employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties that use JSU owned desktops, laptops, servers, applications, mobile and network devices and any other additional equipment, technology resources and services that access sensitive and non-sensitive university data.

5. Policy

   5.1. General Patch Management Policy

      5.1.1. A risk-informed systems patch cycle for all server operating systems (OS) must be scheduled, as appropriate, for JSU Information Systems and related subsystems.

      5.1.2. Any emergency patching process outside of the routine patching schedule must be done according to level of risk, as determined by the system owner in consultation with the JSU Patch Management Team members.

      5.1.3. Servers, services, or applications must be maintained with current OS, application, or security patch levels, as recommended by the software manufacturer and informed by risk, to protect University Information from known information security issues.

      5.1.4. Where and when automated patches cannot be implemented to an end users' system the appropriate IT patch management team members must manually implement the patches

   5.2. Patch Management Roles and Responsibilities

      5.2.1. Management roles and responsibilities and procedures to ensure a quick, effective, and orderly process to managing patches for JSU's information systems and devices are assigned in the table below:

Role	Responsibilities
Chief Information Officer	Review and Approve proposed patch implementation for critical systems
Chief Technology Officer	Review and Approve proposed patch implementation for critical systems
CISO/Cyber Security Officer/Specialist	Lead the PMT in the patch implementation process; proactively identify essential patches that may lead to vulnerabilities
Patch Management Team	Identify and discuss patch releases Test patches; notify the CIO and CTO of adverse effects.

6. Patch Management Process
    - Create and maintain an organizational hardware and software inventory.
    - Identify newly discovered vulnerabilities and security patches using security vulnerability resources (vendor websites, news sources, rss feeds, vendor vulnerability databases).
    - Conduct generic testing of patches in a testing environment
    - Establish a timeline for deploying patches based upon type of updates (critical, non-critical, regularly scheduled maintenance)
    - Roll out the deployment of patches to the production environment
    - Continue to monitor and evaluate patches

7. Exceptions
   The following exceptions for any JSU owned system, software, application or device that cannot be patched to resolve a known vulnerability include 1) the vendor does not have a patch available; 2) the patch provided by vendor creates instability within the system; instability outweighs the risk.

8. Policy Compliance
   8.1. Any JSU employee, vendor(s) and contractor(s) found to have violated this policy may be subject to disciplinary action, up to and including revocation of access privileges, or termination of contract or employment. In addition to University discipline, users may be subject to criminal prosecution under federal, state or local laws; civil liability or both for unlawful use of any IT System.

9. Revision History
    - Policy Created: January 25, 2019
    - Revised: January 10, 2020
    - Revised: August 2, 2021
    - Revised: March 11, 2022
    -