JOLIET JUNIOR COLLEGE 1901

BOARD POLICIES

DIVISION	ADOPTION DATE
X Information Technology	08/2022
POLICY NAME	**REVISIONS**
10.01.08 Patch Management	Revised:

10.01.08 PATCH MANAGEMENT

Purpose

The purpose of this policy is to ensure systems attached to the Joliet Junior College (JJC) network are updated regularly with security patches for known vulnerabilities and exploits. The intention of this practice is to reduce or, if possible, eliminate the vulnerabilities and exploits with minimal impact to College operations.

Scope

This policy applies to all employees and faculty of JJC; including vendors, contractors, partners, students, collaborators, and others doing business with JJC. All will be subject to the provisions of this policy. Any other parties who use, work on, or supply services involving JJC computers, technology systems, and/or data will also be subject to the provisions of this policy.

JJC computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of supporting the educational mission of the College.

The JJC Information Security Office will run vulnerability scans on the network at regular intervals. Additionally, an external vendor will be commissioned to run penetration testing and vulnerability scans to meet our regulatory compliance standards. These findings will be shared regularly with system owners.

Definitions

- **Patches** are an effective way to mitigate software vulnerabilities. Patches may also add new features including security capabilities. New features may also be added through upgrades that bring software or firmware to a newer version. Upgrades can simultaneously fix security and functionality problems in earlier versions.

- **Patch Management** is a process for identifying, acquiring, installing, and verifying software and/or firmware updates on a recurring basis. An effective patch management program ensures all identified information system components are at the latest stable version, as specified and supported by its vendor.
- A **System Owner** is a person determined to have the responsibility for the development, modification, operation, and maintenance of an information system.
- An **Operating System** (OS) is the set of programs used to supply the basic functions of a computer.
- A **device** is defined as any object used to store, process, and/or transfer data.
- A **networked device** is defined as any device that is either permanently or periodically attached to the JJC network.
- **Remediated** is defined as all patches required by the vendor have been applied.
- **Mitigated** is defined as steps that have been taken to protect a device from a particular vulnerability. For example, the device has been removed or otherwise isolated from the network, the NIC card has been removed, or an approved deviation from the required patch process has been approved by the JJC Information Security Office and is documented.

Patch Policy

All networked devices belonging to or managed by JJC departments or other affiliated and partner organizations will be patched with vendor supplied operating system security patches.

Patches will be applied as soon as possible following any necessary testing of the security patches by JJC staff or other partnered organizations. The expectation is that, at a minimum, all critical and high vulnerabilities will be remediated within a maximum of 30 days of discovery. Note this is a maximum, therefore it is imperative that if patches can occur sooner, they should be applied.

New devices must be patched to the current patch level, as defined by the operating system vendor, PRIOR to the device being connected to the production network.

Current patch status for all JJC systems must be communicated to the JJC Information Security Office. Devices that cannot be patched will report the exact mitigation effort to the JJC Information Security Office. Please see more information in the related JJC Vulnerability Report Process.

Out of Support Systems

Vendors routinely cease support and releases of patches for older versions of their products. Upgrades are required to be at the latest version that has ongoing support for patching new vulnerabilities. All device firmware, operating systems, databases, and other software on systems that store, transmit, process and/or receive JJC Data must be under vendor support and recently patched in compliance within 30 days of their findings.

When vendors declare a product to be end of support (or end of life), they will provide an upgrade path or roadmap to replace the legacy product. The expectation is that the JJC system owner/department will upgrade the system to the newest supported version before the end of life/support date expires. Any exception to this policy will need to be approved by both the CIO and the Information Security Office. A lack of funding does not warrant any exception.

All Departments are required to account for the full cost and lifecycle of a product/system that they purchase, implement & own.

Violation of Policy

If it is suspected that this policy is not being adhered to, please report the incident to the JJC Information Security Office. Any exceptions to the policy must be approved in advance by both the Chief Information Officer and the Information Security Office.

Enforcement

Any person or department found to have violated this policy will be subject to disciplinary action as defined by the provisions of Board Policy 10.01.01 Responsible Use of Information Technology.

Exceptions

Limited exceptions to this policy are only permitted in writing by the CIO and the Information Security Office.